Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements

Melanie Cook
Stephen Quinn
David Waltermire
Dragos Prisaca

NIST

National Institute of Standards and Technology

U.S. Department of Commerce

Melanie Cook
Stephen Quinn
David Waltermire
Computer Security Division
Information Technology Laboratory

Dragos Prisaca
G2, Inc.

98   **Reports on Computer Systems Technology**
99
100   The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology
101   (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's
102   measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of
103   concept implementations, and technical analyses to advance the development and productive use of
104   information technology. ITL's responsibilities include the development of management, administrative,
105   technical, and physical standards and guidelines for the cost-effective security and privacy of other than
106   national security-related information in federal information systems.
107

108   **Abstract**

109   This report defines the requirements and associated test procedures necessary for products or modules to
110   achieve one or more Security Content Automation Protocol (SCAP) validations. Validation is awarded
111   based on a defined set of SCAP capabilities by independent laboratories that have been accredited for
112   SCAP testing by the NIST National Voluntary Laboratory Accreditation Program (NVLAP).
113

114   **Keywords**

115   Security Content Automation Protocol (SCAP); SCAP derived test requirements (DTR); SCAP validated
116   tools; SCAP validated products; SCAP validated modules; SCAP validation
117

118

119 **Acknowledgements**

128
129
130 **Audience**

131   This publication is intended for NVLAP accredited laboratories conducting SCAP product and module
132   testing for the program, vendors interested in receiving SCAP validation for their products or modules,
133   and organizations deploying SCAP products in their environments. Accredited laboratories use the
134   information in this report to guide their testing and ensure all necessary requirements are met by a product
135   before recommending to NIST that the product be awarded the requested validation. Vendors may use
136   the information in this report to understand the features that products and modules need in order to be
137   eligible for an SCAP validation. Government agencies and integrators use the information to gain insight
138   into the criteria required for SCAP validated products. The secondary audience for this publication
139   includes end users, who can review the test requirements in order to understand the capabilities of SCAP
140   validated products and gain knowledge about SCAP validation.
141
142
143 **Trademark Information**

144   OVAL and CVE are registered trademarks, and CCE, CPE, and OCIL are trademarks, of The MITRE
145   Corporation.
146
147   Red Hat is a registered trademark of Red Hat, Inc.
148
149   Windows operating system is registered trademark of Microsoft Corporation.
150
151   All other registered trademarks or trademarks belong to their respective organizations.
152

153   **Summary of Changes**

154   The following table details the changes between NISTIR 7511 Revision 3 and NISTIR 7511 Revision 4,
155   which are incorporated in the present document.
156

Date	Type	Change	Page Number
6/26/2015	Editorial	Changed the revision from "3" to "4"	cover page, i, ii
	Editorial	Added new author: "Dragos Prisaca"	cover page, i
	Editorial	Changed secretary name to "Penny Pritzker, Secretary"	i
	Editorial	Changed the date of the document	i
	Substantive	Changed abstract from "This report defines the requirements and associated test procedures necessary for products to achieve one or more Security Content Automation Protocol (SCAP) validations." to 'This report defines the requirements and associated test procedures necessary for products or modules to achieve one or more Security Content Automation Protocol (SCAP) validations."	iii
	Editorial	Added keywords "SCAP validated products; SCAP validated modules"	iii
	Editorial	Updated the Acknowledgements section	iv
	Substantive	Changed "SCAP Product" to "SCAP product and module" in the Audience section	iv
	Substantive	Changed the Trademark Information section from "Windows XP, Windows Vista, and Windows 7 are registered trademarks of Microsoft Corporation." to "Windows® operating system is registered trademark of Microsoft Corporation."	iv
	Substantive	Changed "3.3 Tools" to "3.3 Validation Tools" in the Table of Contents	viii
	Substantive	Changed "3.3.1 SCAP Validation Tool" to "3.3.1 SCAP Validation Tool (SCAPVal)" in the Table of Contents	viii
	Substantive	Added "7. Appendix C— Use of SCAP 1.2 Logo and phrases" to the Table of Contents	viii
	Substantive	Added SCAP Product and Module definitions in the Introduction section	1
	Substantive	Added information about the XML conventions to the section 1.3 Document Conventions	2
	Substantive	Added IR7511 revisions 1, 2, and 3 to the section 1.4 Superseded Validation Programs	4
	Substantive	Added new URL "http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61713" for the XCCDF 1.2 specification in the section 2.1 Extensible Configuration Checklist Document Format (XCCDF)	6
	Substantive	Replaced "Vendor products may seek validation for SCAP 1.2 capabilities for Windows and/or Red Hat platforms. One core SCAP 1.2 capability and two optional capabilities are offered." with "Vendor of products may seek validation for one core and two	10

Date	Type	Change	Page Number
		optional SCAP 1.2 capabilities on one or more platform such as those listed below." in section 3.1 SCAP 1.2 Capabilities and Validations	
	Substantive	Added table with supported platforms in section 3.1 SCAP 1.2 Capabilities and Validations, SCAP Module minor versions are validated	10
	Substantive	Removed the old platforms listed in section 3.1 SCAP 1.2 Capabilities and Validations.	9
	Substantive	Added clarification about supporting new platforms "The SCAP Validation Program may add support for new platforms which will be listed on the SCAP Validation Program web page. For the most current list of available platforms, please refer to http://scap.nist.gov/validation." to section 3.1 SCAP 1.2 Capabilities and Validations	11
	Editorial	Replaced "Product" with "Product/Module" in section 3.1 SCAP 1.2 Capabilities and Validations	11
	Editorial	Changed the example used in section 3.2 Demarcation and Validation Expirations to use future dates.	11
	Editorial	Replaced section name "3.3 Tools" with "3.3Validation Tools"	12
	Editorial	Replaced section name "3.3.1 SCAP Validation Tool" with "3.3.1 SCAP Validation Tool (SCAPVal)"	12
	Substantive	Added "Use of reference implementation tools is not required by the SCAP Validation Program." to section 3.3.2 Reference Implementation Tools	12
	Substantive	Added the <Profile> element to the list XCCDF elements referenced in SCAP.R.1200	18
	Editorial	Replaced "tool" with "product" in SCAP.T.1200.1 and SCAP.T.1200.2	18
	Substantive	Replaced "the Tier IV" with "USGCB" in SCAP.R.1500	19
	Substantive	Added footnote 14 for SCAP.R.1500	19
	Substantive	Replaced "SCAP.V.1500.1: The vendor SHALL provide instructions on how to execute the previously imported valid Tier IV SCAP source data streams." with "SCAP.V.1500.1: The vendor SHALL provide instructions on how to import and execute valid SCAPUSGCB source data streams."	20
	Editorial	Corrected typo in footnote 12	17
	Substantive	Added SCAP.V.1500.2	20
	Substantive	Changed the instructions for the section Required Test Procedures of SCAP.R.1500	20
	Substantive	Added "All the applicable USGCB source data streams published in the official National Checklist Program Repository should be used for testing this requirement: http://checklists.nist.gov." in section "Required Test Procedures" of SCAP.R.1500.	20
	Substantive	Removed Tier IV source data streams listed in the section Required Test Procedures of SCAP.R.1500	20

Date	Type	Change	Page Number
	Substantive	Changed "SCAP.T.1500.1: The tester SHALL evaluate the compliant target platforms, in a domain connected configuration for Windows and standalone configuration for Red Hat, and compare the pass/fail results from the product to the expected results, ensuring the actual results match the expected results." to "SCAP.T.1500.1: The lab or the vendor SHALL evaluate the compliant target platforms, in a domain connected configuration for Windows and standalone configuration for other platforms (i.e., RHEL, Mac OS X, Unix, etc.), and compare the pass/fail results from the product to the expected results, ensuring the actual results match the expected results. If the testing is performed by the vendor, the source data streams, the scan results, and their hashes will be submitted to the lab for verification."	20
	Substantive	Added footnote 15: "The hashes SHALL comply with Annex A: Approved Security Functions of FIPS 140-2 publication."	20
	Substantive	Added SCAP.T.1500.2	20
	Substantive	Added new requirement SCAP.R.1510	20
	Substantive	Changed "Tier IV content" to "USGCB checklist" for SCAP.R.1600	21
	Substantive	Replaced "SCAP.R.1700: The product SHALL be able to process the content that is representative of content published at Tier III and the OVAL repository which is associated with the platforms for which validation is being sought." with "SCAP.R.1700: The product SHALL be able to correctly process the content that is representative of content published at Tier III, Tier IV, and the OVAL repository16 which is associated with the platforms for which validation is being sought."	21
	Substantive	Added footnote 17: "The OVAL repository is hosted by MITRE Corporation: https://oval.mitre.org/repository/"	21
	Substantive	Changed "XCCDF <Benchmark>, <Group>, or <Rule>" to "XCCDF <Benchmark>, <Profile>, <Group>, or <Rule>" in SCAP.R.1800.	22
	Editorial	Changed "tool" to "product" in SCAP.T.1800.1.	22
	Substantive	Changed "SCAP.R.1900: The product SHALL be able to correctly evaluate a valid OVAL Definition file and external variable file, where the contents of the OVAL Definition file are consistent with the normative guidance specified in NIST SP 800-126 Revision 1, against target systems of the target platform type and produce a result file for each definition using the OVAL XML Full Results expressed as Single Machine Without System Characteristics, Single Machine With System Characteristics, or Single Machine With Thin Results." to "SCAP.R.1900: The product SHALL be able to correctly evaluate a valid OVAL Definition file and external variable file, where the contents of the OVAL Definition file are consistent with the normative guidance specified in NIST SP 800-126 Revision 1, against target systems of the target platform type and produce a result file for each definition using the OVAL XML Full Results expressed as Single Machine Without System	22

Date	Type	Change	Page Number
		Characteristics, Single Machine With System Characteristics, and Single Machine With Thin Results." in SCAP.R.1900.	
	Editorial	Changed "tool" to "product" in SCAP.T.1900.1.	22
	Substantive	Changed "SCAP.R.2000: The product SHALL be able to correctly evaluate a valid OVAL Definition file that is part of an SCAP data stream, where the contents of the OVAL definition file are consistent with the normative guidance specified in NIST SP 800-126 Revision 2, against target systems of the target platform type and produce a result file for each definition using the OVAL XML Full Results expressed as Single Machine Without System Characteristics, Single Machine With System Characteristics, or Single Machine With Thin Results. " to "SCAP.R.2000: The product SHALL be able to correctly evaluate a valid OVAL Definition file that is part of an SCAP data stream, where the contents of the OVAL definition file are consistent with the normative guidance specified in NIST SP 800-126 Revision 2, against target systems of the target platform type and produce a result file for each definition using the OVAL XML Full Results expressed as Single Machine Without System Characteristics, Single Machine With System Characteristics, and Single Machine With Thin Results." In SCAP.R.2000.	23
	Substantive	Removed "For SCAP.T.2000.5, the vendor SHALL indicate how two or more values can be specified for a variable used by one OVAL Definition." from section Required Vendor Information - SCAP.V.2000.1.	23
	Editorial	Changed "tool" to "product" in SCAP.T.2000.1.	23
	Substantive	Removed "SCAP.T.2000.5: When an OVAL Definition has been evaluated more than once on a single target system, each time with different values for the variables, the tester SHALL validate that the OVAL XML Full Results file includes unique variable instance values for each individual case."	23
	Editorial	Changed "tool" to "product" in SCAP.T.2100.1.	24
	Editorial	Changed "tool" to "product" in SCAP.T.2200.1.	24
	Substantive	Changed "SCAP.R.3600" to "SCAP.R.2930" in SCAP.T.2300.1.	24
	Substantive	Changed "SCAP.R.3600" to "SCAP.R.2930" in SCAP.T.2400.1.	24
	Editorial	Changed "tool" to "product" in SCAP.T.2600.1.	26
	Substantive	Changed "SCAP.R.4400" to "SCAP.R.2920" in SCAP.T.2700.1.	26
	Substantive	Removed "and/or patch definitions" and changed "SCAP.R.4400" to "SCAP.R.2920" in SCAP.T.2800.1.	27
	Substantive	Added new requirement SCAP.R.2910	27
	Substantive	Added new requirement SCAP.R.2920	28
	Substantive	Added new requirement SCAP.R.2930	28
	Substantive	Added new requirement SCAP.R.2940	28
	Editorial	Changed "tool" to "product" in SCAP.T.3000.1.	29
	Substantive	Added new requirement SCAP.R.3005	28

Date	Type	Change	Page Number
	Substantive	Added new requirement SCAP.R.3010	29
	Editorial	Changed "tool" to "product" in SCAP.T.3200	30
	Editorial	Changed "tool" to "product" in SCAP.T.3300.1.	31
	Editorial	Changed "tool" to "product" in SCAP.T.3400	31
	Editorial	Changed "tool" to "product" in section 5. Derived Test Requirements for Specific Capabilities	36
		Added the following entries to Table 5-1. Required SCAP Components for Each SCAP Capability: SCAP.R.1510, SCAP.R.2910, SCAP.R.2920, SCAP.R.2930, SCAP.R.2940, and SCAP.R.3010	36/37
	Substantive	Changed "Table 5-2 lists the OVAL tests used for testing the ACS SCAP 1.2 capability." to "The list of OVAL tests used for testing the ACS SCAP 1.2 capability is published on the SCAP Validation Program web page http://scap.nist.gov/validation." in section 5. Derived Test Requirements for Specific Capabilities	38
	Editorial	Removed Table 5.2 OVAL Tests	38
	Editorial	Changed "tool" to "product" in Appendix A.	39
	Editorial	Added SCAP Module definition in Appendix A.	40
	Editorial	Removed definition for Reference Product in Appendix A.	40
	Editorial	Added Appendix C	43

157

158   **Table of Contents**

195

196 **1.   Introduction**

197   The National Institute of Standards and Technology (NIST) Security Content Automation Protocol
198   (SCAP) Validation Program tests the ability of products and modules to use the features and functionality
199   available through SCAP and its components. SCAP 1.2 consists of a suite of specifications for
200   standardizing the format and nomenclature by which security software communicates information about
201   software flaws and security configurations. The standardization of security information facilitates
202   interoperability and enables predictable results among disparate SCAP enabled security software. The
203   SCAP Validation Program provides vendors an opportunity to have independent verification that security
204   software correctly processes SCAP expressed security information and provides standardized output.
205   Industry and government end users benefit from the SCAP Validation Program by having assurance that
206   SCAP validated products have undergone independent testing and met all requirements defined in this
207   document.

208   The validation program supports the U.S. Office of Management and Budget (OMB) Memorandum M-
209   08-22 to Federal CIOs [OMB M-08-22]. This memorandum states, "Both industry and government
210   information technology providers must use SCAP validated tools with FDCC Scanner capability to certify
211   their products operate correctly with FDCC configurations and do not alter FDCC settings. Agencies will
212   use SCAP tools to scan for both FDCC configurations and configuration deviations approved by
213   department or agency accrediting authority. Agencies must also use these tools when monitoring use of
214   these configurations as part of FISMA continuous monitoring."[1] The checklist portion of the FDCC
215   mandate is now referred to as the United States Government Configuration Baseline (USGCB), and the
216   FDCC Scanner capability has evolved and is now referred to as the Authenticated Configuration Scanner
217   (ACS) capability.[2]

218   Under the SCAP Validation Program, independent laboratories are accredited by the NIST National
219   Voluntary Laboratory Accreditation Program (NVLAP). Accreditation requirements are defined in NIST
220   Handbook 150, *National Voluntary Laboratory Accreditation Program: Procedures and General*
221   *Requirements* [NIST HB 150] and NIST Handbook 150-17, *NVLAP Cryptographic and Security Testing*
222   [NIST HB 150-17]. More information about NVLAP can be found at http://www.nist.gov/nvlap/.

223   Independent laboratories conduct the tests defined in this document on products and deliver the results to
224   NIST. Based on the independent laboratory test report, the SCAP Validation Program then validates the
225   product under test. The validation certificates awarded to vendor's products are publicly posted on the
226   NIST SCAP Validated Products web page (http://nvd.nist.gov/scapproducts.cfm).[3] An information
227   technology (IT) vendor can obtain one or more validations for a product. These validations are based on
228   the test requirements defined in this document. Products are validated in the context of a particular SCAP
229   capability.[4]

230   An SCAP product is defined as a software application that has one or more capabilities and an SCAP
231   module is defined as an embedded software component of a product or application, or a complete product
232   in-and-of-itself that has one or more capabilities. Unless otherwise stated herein, the term "product" refers
233   to either a "product" or "module" under test.

---

[1]   [OMB M-08-22, p.2]
[2]   http://usgcb.nist.gov
[3]   The SCAP Validation Program does not provide physical certificates to the participating vendors.
[4]   The SCAP Validation Program defines SCAP capability as "a specific function or functions of a product or module".
       Further information can be found in Section 3.

234 **1.1   Purpose and Scope**

235   The purpose of this report is to define the SCAP 1.2 Validation Program Derived Test Requirements. This
236   report gives an introduction to the SCAP 1.2 Validation Program and documents the requirements for
237   SCAP 1.2 product and module validations. Future versions of the SCAP Validation Program will be
238   defined in revisions of this report, each clearly labeled with a revision number and the appropriate SCAP
239   version number.

240   **1.2   Document Structure**

241   The remainder of this document is organized into the following major sections:
242   •   Section 2 describes SCAP and its component specification versions referenced in the SCAP 1.2
243   validation program,
244   •   Section 3 describes the validation process,
245   •   Section 4 defines the derived test requirements,
246   •   Section 5 maps the derived test requirements to SCAP capabilities,
247   •   Appendix A—Terms and Definitions lists terms and definitions,
248   •   Appendix B—Acronyms lists acronyms,
249   •   Appendix C—Use of SCAP 1.2 Logo and phrases discusses the use of the SCAP 1.2 logo and
250   phrases, and
251   •   Appendix D—References includes a list of references.
252
253   **1.3   Document Conventions**

254   Throughout this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL
255   NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
256   document are to be interpreted as described in the Internet Engineering Task Force (IETF) Request for
257   Comments (RFC) 2119 [RFC 2119].
258
259   Some of the requirements and conventions used in this document reference Extensible Markup Language
260   (XML) content [XMLS]. These references come in two forms, inline and indented. An example of an
261   inline reference is: a `<cpe2_dict:cpe-item>` may contain `<cpe2_dict:check>` elements that
262   reference OVAL Definitions.

263   In this example the notation `<cpe2_dict:cpe-item>` can be replaced by the more verbose
264   equivalent "the XML element whose qualified name is `cpe2_dict:cpe-item`".

266   An example of an indented reference is:

267   References to OVAL Definitions are expressed using the following format:

268   `<cpe2_dict:check system=`
269   `"http://oval.mitre.org/XMLSchema/oval-definitions-5"`
270   `href="`*Oval_URL*`">[`*Oval_inventory_definition_id*`]`
271   `</cpe2_dict:check>`.

272   The general convention used when describing XML attributes within this document is to reference the
273   attribute as well as its associated element including the namespace alias, employing the general form
274   `"@attributeName` for the `<prefix:localName>"`.

275   Indented references are intended to represent the form of actual XML content. Indented references
276   represent literal content by the use of a `fixed-length font`, and parametric (freely replaceable)

277 content by the use of an *italic font*. Square brackets '[]' are used to designate optional content. Thus
278 "[*Oval_inventory_definition_id*]" designates optional parametric content.

279 Both inline and indented forms use qualified names to refer to specific XML elements. A qualified name
280 associates a named element with a namespace. The namespace identifies the XML model, and the XML
281 schema is a definition and implementation of that model. A qualified name declares this schema to
282 element association using the format '*prefix*:*element-name*'. The association of prefix to namespace is
283 defined in the metadata of an XML document and varies from document to document. In this
284 specification, the conventional mappings listed in Table 1-1.-1 are used.
285
286   Table 1-1. Conventional XML Mappings[5]
287

Prefix	Namespace	Schema
cpe2	http://cpe.mitre.org/language/2.0	Embedded CPE references
cpe2-dict	http://cpe.mitre.org/dictionary/2.0	CPE dictionaries
xccdf	http://checklists.nist.gov/xccdf/1.2	XCCDF policy documents
xml	http://www.w3.org/XML/1998/namespace	Common XML attributes

288
289
290
291 1.4   Superseded Validation Programs

292 This publication supersedes the draft *Security Content Automation Protocol (SCAP) Validation Program*
293 *Test Requirements Version 1.0* released in August 2008, the *Security Content Automation Protocol*
294 *(SCAP) Version 1.0 Validation Program Test Requirements* released in April 2009, the *Security Content*
295 *Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements* released in September
296 2010, the *Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test*
297 *Requirements Update* released in January 2011, and the *Security Content Automation Protocol (SCAP)*
298 *Version 1.2 Validation Program Test Requirements* revisions 1, 2, and 3.

---

[5] For a complete list of mappings, please refer to [NIST SP 800-126 R2].

2. SCAP 1.2 Component Specification Versions

299

300 For all test requirements that reference particular specifications, the versions indicated in this section
301 SHOULD be used and are derived primarily from the SCAP 1.2 as defined in NIST Special Publication
302 (SP) 800-126 Revision 2 [NIST SP 800-126 R2].

303 SCAP is a suite of specifications established by NIST for expressing and manipulating security data in
304 standardized ways. Adoption of SCAP facilitates an organization's automation of continuous monitoring,
305 vulnerability management, and security policy compliance evaluation reporting.

306 The component specifications that comprise SCAP 1.2 are as follows:

307 ■ Extensible Configuration Checklist Description Format (XCCDF) 1.2, an Extensible Markup
308 Language (XML) specification for structured collections of security configuration rules used by
309 operating system (OS) and application platforms;

310 ■ Open Vulnerability and Assessment Language (OVAL) 5.10.1, an XML specification for exchanging
311 technical details on how to check systems for security-related software flaws, configuration issues,
312 and software patches;

313 ■ Open Checklist Interactive Language (OCIL) 2.0, a language for representing checks that collect
314 information from people or from existing data stores made by other data collection efforts;

315 ■ Common Configuration Enumeration (CCE) 5, a dictionary of names for software security
316 configuration issues (e.g., access control settings, password policy settings);

317 ■ Common Platform Enumeration (CPE) 2.3, a naming convention for hardware, OS, and application
318 products;

319 ■ Common Vulnerabilities and Exposures (CVE), a dictionary of names for publicly known security-
320 related software flaws;

321 ■ Common Vulnerability Scoring System (CVSS) 2.0, a method for classifying characteristics of
322 software flaws and assigning severity scores based on these characteristics;

323 ■ Common Configuration Scoring System (CCSS) 1.0, a system for measuring the relative severity of
324 system security configuration issues;

325 ■ Asset Identification 1.1, a format for uniquely identifying assets based on known identifiers and/or
326 known information about the assets;

327 ■ Asset Reporting Format (ARF) 1.1, a format for expressing the transport format of information about
328 assets and the relationships between assets and reports; and

329 ■ Trust Model for Security Automation Data (TMSAD) 1.0, a specification for using digital signatures
330 in a common trust model applied to other security automation specifications.

331 The SCAP specification describes the SCAP components at a high level and how the components relate
332 to each other within the context of SCAP. The SCAP specification does not define the SCAP
333 components in detail; each component has its own standalone specification document or reference. The
334 SCAP components were created and are maintained by several entities, including NIST, the MITRE
335 Corporation, the National Security Agency (NSA), and the Forum of Incident Response and Security
336 Teams (FIRST).

337   NIST provides SCAP content, such as vulnerability and product enumeration identifiers, through a
338   repository supplied by the National Vulnerability Database (NVD).[6] All of the content in NVD and the
339   SCAP specification are freely available from NIST. SCAP content is also created and made available by
340   non-U.S. government organizations through the National Checklist Program (NCP).[7] More information
341   about SCAP can be found at http://scap.nist.gov/.

342   **2.1   Extensible Configuration Checklist Document Format (XCCDF)**

343   Definition: XCCDF is an XML-based language for representing security checklists, benchmarks, and
344   related documents in a machine-readable form. An XCCDF document represents a structured collection
345   of security configuration rules for one or more applications and/or systems. The XCCDF specification
346   also defines a data model and format for storing the results of benchmark compliance testing.

347   Version: 1.2

348   Specification: http://csrc.nist.gov/publications/nistir/ir7275-rev4/NISTIR-7275r4.pdf [NISTIR 7275 R4]
349   http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61713

350   Schema Location: http://scap.nist.gov/schema/xccdf/1.2/xccdf_1.2.xsd

351   **2.2   Open Vulnerability and Assessment Language (OVAL)**

352   Definition: OVAL is an XML-based language used for communicating the details of vulnerabilities,
353   patches, security configuration settings, and other machine states in a machine-readable form. There is
354   also the OVAL Power Shell Extension, a method for examining the configuration of Microsoft products.

355   Version: 5.10.1

356   Specification: http://oval.mitre.org/

357   Schema Location: http://oval.mitre.org/language/download/schema/version5.10/index.html

358   **2.3   Open Checklist Interactive Language (OCIL)**

359   Definition: OCIL defines a framework for expressing a set of questions to be presented to a user and
360   corresponding procedures to interpret responses to these questions.
361
362   Version: 2.0
363
364   Specification: http://csrc.nist.gov/publications/nistir/ir7692/nistir-7692.pdf [NISTIR 7692]
365
366   Schema Location: http://scap.nist.gov/schema/ocil/2.0/ocil-2.0.xsd
367
368   **2.4   Common Configuration Enumeration (CCE)**

369   Definition: CCE is a format for describing system configuration issues to facilitate correlation of
370   configuration data across multiple information sources and tools.

371   Version: 5

---

[6]   http://nvd.nist.gov
[7]   http://checklists.nist.gov

372   Specification: http://cce.mitre.org/

373   Dictionary: http://cce.mitre.org/lists/cce_list.html

374   **2.5   Common Platform Enumeration (CPE)**

375   Definition: CPE is a standardized method of describing and identifying classes of applications, operating
376   systems, and hardware devices present among an enterprise's computing assets. CPE 2.3 is defined
377   through a set of specifications in a stack-based model.

378   **2.5.1   CPE.Naming**

379   Definition: The Naming specification defines the logical structure of Well-Formed Names (WFNs).
380
381   Version: 2.3
382
383   Specification: http://csrc.nist.gov/publications/nistir/ir7695/NISTIR-7695-CPE-Naming.pdf [NISTIR
384   7695]
385
386   Schema Location: http://scap.nist.gov/schema/cpe/2.3/cpe-naming_2.3.xsd
387
388   **2.5.2   CPE.Name Matching**

389   Definition: The Name Matching specification defines the procedures for comparing WFNs to each other
390   with the purpose of determining whether they refer to some or all of the same products.
391
392   Version: 2.3
393
394   Specification: http://csrc.nist.gov/publications/nistir/ir7696/NISTIR-7696-CPE-Matching.pdf [NISTIR
395   7696]
396
397   **2.5.3   CPE.Dictionary**

398   Definition: The Dictionary specification defines the concept of a CPE dictionary, which is a repository of
399   CPE names and metadata, with each name identifying a single class of IT product. The Dictionary
400   specification defines processes for using the dictionary, such as how to search for a particular CPE name
401   or look for dictionary entries that belong to a broader product class. Also, the Dictionary specification
402   outlines all the rules that dictionary maintainers MUST follow when creating new dictionary entries and
403   updating existing entries.
404
405   Version: 2.3
406
407   Specification: http://csrc.nist.gov/publications/nistir/ir7697/NISTIR-7697-CPE-Dictionary.pdf [NISTIR
408   7697]
409
410   Schema Locations: http://scap.nist.gov/schema/cpe/2.3/cpe-dictionary_2.3.xsd
411   http://scap.nist.gov/schema/cpe/2.3/cpe-dictionary-extension_2.3.xsd
412

413 **2.5.4 CPE.Applicability Language**

414 Definition: The Applicability Language specification defines a standardized structure for forming
415 complex logical expressions out of WFNs. These expressions, also known as applicability statements, are
416 used to tag checklists, policies, guidance, and other documents with information about the product(s) to
417 which the documents apply.

418 Version: 2.3

419 Specification: http://csrc.nist.gov/publications/nistir/ir7698/NISTIR-7698-CPE-Language.pdf [NISTIR
420 7698]

421 Schema Location: http://scap.nist.gov/schema/cpe/2.3/cpe-language_2.3.xsd

422 **2.6 Common Vulnerabilities and Exposures (CVE)**

423 Definition: CVE is a format to describe publicly known information security vulnerabilities and
424 exposures. Using this format, new CVE IDs will be created, assigned, and referenced in content on an as-
425 needed basis without a version change.

426 Version: N/A

427 Specification: http://cve.mitre.org/

428 Dictionary: http://nvd.nist.gov/

429 **2.7 Common Vulnerability Scoring System (CVSS)**

430 Definition: CVSS is a scoring system that provides an open framework for determining the relative
431 severity of software flaw vulnerabilities and a standardized format for communicating vulnerability
432 characteristics.

433 Version: 2.0

434 Specification: http://csrc.nist.gov/publications/nistir/ir7435/NISTIR-7435.pdf [NISTIR 7435]

435 CVSS Base Scores: http://nvd.nist.gov/

436 **2.8 Common Configuration Scoring System (CCSS)**

437 Definition: CCSS is a set of measures of the severity of software security configuration issues.
438
439 Version: 1.0
440
441 Specification: http://csrc.nist.gov/publications/nistir/ir7502/nistir-7502_CCSS.pdf [NISTIR 7502]
442
443 **2.9 Asset Identification**

444 Definition: The Asset Identification specification provides the necessary constructs to uniquely identify
445 assets based on known identifiers and/or known information about the assets. This specification describes
446 the purpose of asset identification, a data model for identifying assets, methods for identifying assets, and

447 guidance on how to use asset identification. It also identifies a number of known use cases for asset
448 identification.
449
450 Version: 1.1
451
452 Specification: http://csrc.nist.gov/publications/nistir/ir7693/NISTIR-7693.pdf [NISTIR 7693]
453
454 Schema Location: http://scap.nist.gov/schema/asset-identification/1.1/asset-identification_1.1.0.xsd
455

2.10 Asset Reporting Format (ARF)

457 Definition: ARF is a data model to express the transport format of information about assets, and the
458 relationships between assets and reports. The standardized data model facilitates the reporting,
459 correlating, and fusing of asset information throughout and between organizations.
460
461 Version: 1.1
462
463 Specification: http://csrc.nist.gov/publications/nistir/ir7694/NISTIR-7694.pdf [NISTIR 7694]
464
465 Schema Location: http://scap.nist.gov/schema/asset-reporting-format/1.1/asset-reporting-format_1.1.0-
466 rc1.xsd
467

2.11 Trust Model for Security Automation Data (TMSAD)

469 Definition: TMSAD is a data model for establishing trust for security automation data.
470
471 Version: 1.0
472
473 Specification: http://csrc.nist.gov/publications/nistir/ir7802/NISTIR-7802.pdf [NISTIR 7802]
474
475 Schema Location: http://scap.nist.gov/schema/tmsad/1.0/tmsad_1.0.xsd
476

477 **3.   Validation Process**

478 With the SCAP Validation Program, SCAP accredited laboratories conduct the tests defined in this
479 document on products and deliver the test report to NIST. NIST reviews the test report and determines
480 whether the product has successfully fulfilled all requirements for SCAP validation. Upon successful
481 completion of all requirements, the SCAP Validation Program then validates the product based on the
482 independent laboratory test report. SCAP validated products and modules are publicly posted on the NIST
483 SCAP Validated Products web page at http://nvd.nist.gov/scapproducts.cfm.

484 This section of the document covers the validation process. Section 3.1 discusses SCAP 1.2 capabilities
485 and validations. Section 3.2 addresses demarcation and validation expirations. Finally, Section 3.3
486 discusses reference implementation tools.

487 **3.1   SCAP 1.2 Capabilities and Validations**

488 Vendor products may seek validation for one core and two optional SCAP 1.2 capabilities on one or more
489 platform such as those listed below.

490 **SCAP Capabilities**

491   • Authenticated Configuration Scanner (ACS) core SCAP 1.2 capability
492   o CVE option (optional CVE support may be combined with ACS)
493   o OCIL option (optional OCIL support may be combined with ACS)
494
495 **NOTE:** The ACS capability includes the FDCC Scanner functionality that is mentioned in Office of
496 Management and Budget (OMB) memorandum M-08-22, *Guidance on the Federal Desktop Core*
497 *Configuration (FDCC)* [OMB M-08-22] and the USGCB Scanner previously offered in the SCAP 1.0
498 validation program.

499 **Platforms**

Microsoft Windows
Microsoft Windows XP Professional with Service Pack 3
Microsoft Windows Vista with Service Pack 2 or later
Microsoft Windows 7 SP1 or later, 32-bit edition
Microsoft Windows 7 SP1 or later, 64-bit edition
Microsoft Windows 8.1 SP0 or later, 32-bit edition
Microsoft Windows 8.1 SP0 or later, 64-bit edition
Microsoft Windows Server 2012 R2 SP0 or later, 64-bit edition
Red Hat Enterprise Linux
Red Hat Enterprise Linux 5, 32-bit edition
Red Hat Enterprise Linux 5, 64-bit edition
Red Hat Enterprise Linux 6, 32-bit edition
Red Hat Enterprise Linux 6, 64-bit edition

500

501 The SCAP Validation Program is not inherently limited to the platforms listed above and NIST reserves
502 the right to add or remove platforms in future updates to the SCAP 1.2 Validation Program. The SCAP
503 Validation Program may add support for new platforms which will be listed on the SCAP Validation
504 Program web page. For the most current list of available platforms, please refer to
505 http://scap.nist.gov/validation.

506 Validations will be awarded to major product versions for SCAP capabilities and platforms supported.
507 Vendors must provide a description of their product versioning method in order to define how major
508 releases are numbered for the product entering the validation process. In general, validations will be
509 awarded to major releases of products; however, if a minor release modifies the SCAP component of the
510 product, then the vendor should enter validation for the minor release.

511 Validations will be awarded to SCAP module minor version number. Vendors must provide a versioning
512 statement that describes how module versions are assigned. As with products, any modification of the
513 SCAP component requires revalidation. Validated products will be listed on the SCAP Validated
514 Products web page to include, but not limited to the following corresponding information:

515 • Product/module vendor or manufacturer name
516 • Product/module name
517 • Product/module major version validated
518 • Product/module version tested (full identifier at the time of testing)
519 • Platforms tested
520 • SCAP Capabilities
521 • Validation number
522 • Validation date
523 • Validation test suite version used for testing
524

525 **3.2 Demarcation and Validation Expirations**

526 The SCAP Validation Program recognizes the need for a clear demarcation point for end users, product
527 vendors, the standards body and NVLAP accredited labs in order to develop, test, and deploy efficiently.
528 The SCAP Validation Program also recognizes that SCAP component specifications, standards, and
529 products typically change over time and employ a variety of versioning schemes for identifying different
530 releases.
531

532 The final release date of NIST IR 7511 for the next version of SCAP[8] determines the end of the SCAP 1.2
533 Validation Program and the expiration date for SCAP 1.2 product validations. The SCAP 1.2 Validation
534 Program will end 15 months after the final release of NIST IR 7511 for the next SCAP version. SCAP 1.2
535 product validations will expire 12 months after the SCAP 1.2 Validation Program ends. For example, if
536 NIST IR 7511 for SCAP 1.3[9] is finalized on January 1, 2017, the SCAP 1.2 Validation Program would
537 end on March 31, 2018. All SCAP 1.2 validated products would expire on March 31, 2019. The new
538 SCAP 1.3 Validation Program would begin April 1, 2017.[10]
539

540 This document identifies a specific set of SCAP component specifications as described in Section 2 and
541 the associated Derived Test Requirements (DTRs) as described in Section 4. Minor updates to SCAP

---

[8] The current version of SCAP is 1.2.
[9] This statement explains the revision cycle. The next release of SCAP may or may not be numbered 1.3, and the release date in this example is hypothetical.
[10] See http://scap.nist.gov/timeline.html for more information about the SCAP release cycle.

542   component specifications and products do not invalidate currently validated products. Major changes in
543   functionality, including support for new SCAP technologies, may require product revalidation.
544
545   **3.3   Validation Tools**

546   The SCAP Validation Program uses several reference implementation tools that aid in the development
547   and testing of SCAP products. The SCAP Validation (SCAPVal) Tool may be used for checking the
548   correctness of SCAP data streams; SCAPVal is required during formal SCAP validation testing.
549   Reference implementation tools may be used to process SCAP content; these tools are not required during
550   formal SCAP validation testing. The SCAP Validation Tool and reference implementation tools are
551   discussed in more detail below.
552
553   **3.3.1   SCAP Validation Tool**

554   The SCAP Validation Tool (SCAPVal) validates the correctness of an SCAP data stream for a particular
555   use case according to what is defined in SP 800-126. The SCAPVal output provides information about
556   whether an SCAP data stream (.zip file) conforms to conventions and recommendations outlined in NIST
557   SP 800-126 Revision 2 [NIST SP 800-126 R2].
558
559   SCAPVal provides the following functions:
560   • Validates the data stream according to one of the use cases for an SCAP-validated product listed
561   in Section 5 of [NIST SP 800-126 R2], namely Compliance Checking, Vulnerability Scanning, or
562   Inventory Scanning.
563   • Checks components and data streams against appropriate schemas.
564   • Uses Schematron to perform additional checks within and across component data streams.
565   • Produces validation results that convey all error and warning conditions detected; results are
566   output in both XML and HTML formats.
567   For a listing of the SCAP requirements, refer to the SCAP Version 1.0 Requirements Matrix, SCAP
568   Version 1.1 Requirements Matrix, and SCAP Version 1.2 Requirements Matrix included with the tool.
569   SCAPVal may be downloaded from http://scap.nist.gov/revision/index.html.
570
571   **3.3.2   Reference Implementation Tools**

572   Reference implementation tools or interpreters are open source tools that process SCAP data streams.
573   Several interpreters are available with varying degrees of support across platforms. Each interpreter is
574   command line and all have readme files providing usage guidance. Use of reference implementation tools
575   is not required by the SCAP Validation Program.
576
577   The SCAP interpreter is an open source Java application that scans a system based on the requirements
578   defined in [NIST SP 800-126 R2]. This application uses the XCCDF interpreter, the OVAL interpreter,
579   and the OCIL interpreter when processing SCAP data streams. SCAP versions 1.0, 1.1, and 1.2 are
580   supported. The SCAP interpreter is available on SourceForge at http://sourceforge.net/projects/scapexec/.
581
582   The XCCDF interpreter is an open source application for performing system analysis and report
583   generation using the XCCDF format. This application will process XCCDF and OVAL files. The
584   application is available on SourceForge at http://sourceforge.net/projects/xccdfexec/.
585
586   The OVAL interpreter (OVAL DI) is an open source application that demonstrates the evaluation of
587   OVAL definitions. This reference implementation collects system information, evaluates it, and generates
588   a detailed OVAL Results file. The OVAL interpreter is available on SourceForge at
589   http://sourceforge.net/projects/ovaldi/.

590
591   The OCIL interpreter (OCIL QI) is an open source Java GUI application that demonstrates how an OCIL
592   document can be evaluated. It guides the end user in completing questionnaires, viewing, and computing
593   results. This application is available on SourceForge at http://sourceforge.net/projects/interactive/.
594

595 **4. Derived Test Requirements**

596 This section contains the test requirements for each of the SCAP components for the purpose of allowing
597 individual validation of each SCAP component within a product. Version information and download
598 location, listed in Section 2, SHOULD be referenced to ensure that the correct version is being used prior
599 to testing. SCAP-specific requirements are found in Section 5.

600 Each DTR includes the following information:

601 ■ The DTR name: comprised of the acronym followed by ".R" to denote it is a requirement, and then
602 the requirement number.

603 ■ SCAP Capability (summarized in Table 5-1) where

604 o ACS = Authenticated Configuration Scanner

605 o CVE = Optional CVE Support when combined with ACS

606 o OCIL = Optional OCIL Support when combined with ACS

607 ■ Required vendor information: states required information vendors MUST provide to the testing lab
608 for the test to be conducted.

609 ■ Required test procedure(s): defines one or more tests that the testing laboratory will conduct to
610 determine the product's ability to meet the stated requirement.

611 The derived requirements are organized into the following major categories:

612 1. Assertions – Statements made by the products (in its documentation) that indicate what the
613 product does (or does not) do relative to SCAP and its components (see Section 4.1)

614 2. Input Processing and Correctness – Those requirements that define the processing of SCAP
615 source data streams and their major permutations (e.g., various source data stream tests such as
616 source data streams with multiple benchmarks, legacy data streams, and signed data streams) (see
617 Section 4.2)

618 3. Results Production – Those requirements that define how products will be assessed for their
619 ability to produce valid SCAP results (see Section 4.3)

620

621

4.1   SCAP Assertions

This section addresses the assertions that vendors MUST make about the products seeking validations relative to SCAP and its component specifications as defined in Section 2.

SCAP.R.100: The product's documentation (printed or electronic) MUST assert that it uses SCAP and its component specifications and explain relevant details to the users of the product.

      SCAP Capability: ☑ ACS   ☐ CVE   ☐ OCIL

      Required Vendor Information:

      SCAP.V.100.1: The vendor SHALL indicate where in the product documentation information regarding the use of SCAP and its components can be found. This MAY be a physical document or a static electronic document (e.g., a PDF or help file).

      Required Test Procedures:

      SCAP.T.100.1: The tester SHALL visually inspect the product documentation to verify that information regarding the product's use of SCAP and its components is present and verify that the SCAP documentation is in a location accessible to any user of the product. This test does not involve judging the quality of the documentation or its accuracy.

SCAP.R.200: The vendor MUST assert that the product implements SCAP and its component specifications and provide a high-level summary of the implementation approach as well as a statement of backward compatibility with earlier versions of SCAP and related components.

      SCAP Capability: ☑ ACS   ☐ CVE   ☐ OCIL

      Required Vendor Information:

      SCAP.V.200.1: The vendor SHALL provide to the lab a separate, 150 to 2500 word explanation written in the English language asserting that the product implements SCAP and its component specifications for the capabilities claimed in Table 5-1. This document SHALL include a high-level summary of the implementation approach and an assertion of backwards compatibility with SCAP 1.0 and SCAP 1.1. This content will be used on NIST web pages to explain details about each validated product and thus SHOULD contain only information that is to be publicly released.

      Required Test Procedures:

      SCAP.T.200.1: The tester SHALL inspect the provided documentation to verify that the documentation asserts that the product implements SCAP and its component specifications and provides a high-level summary of the implementation approach and an assertion of backwards compatibility with SCAP 1.0 and SCAP 1.1. This test does not judge the quality or accuracy of the documentation, nor does it test how thoroughly the product implements SCAP or backwards compatibility with previous versions.

      SCAP.T.200.2: The tester SHALL verify that the provided documentation is an English language document consisting of 150 to 2500 words.

658 **SCAP.R.300: The SCAP capabilities claimed by the vendor for the product under test MUST**
659 **match the scope of the product's asserted capabilities for the target platform.**

660   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

661   **Required Vendor Information:**

662   SCAP.V.300.1: The vendor SHALL indicate the defined SCAP capabilities (one or more) for
663   which their product is being tested.

664   **Required Test Procedures:**

665   SCAP.T.300.1: The tester SHALL ensure that all tests associated with the asserted SCAP
666   capabilities of the product are conducted.

667   SCAP.T.300.2: The tester SHALL review product documentation to ensure that the product has
668   implemented the SCAP capabilities for which it is being tested (e.g., Authenticated Configuration
669   Scanner).

670 **4.2   SCAP Source Data Stream Processing and Correctness**

671 This section addresses the ability of a product to correctly process SCAP source data streams.
672
673 **SCAP.R.400: The product SHALL be able to import SCAP source data streams for the target**
674 **platform and correctly load the included Rules and their associated Check System Definitions,**
675 **rejecting any invalid content.**

676   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

677   **Required Vendor Information:**

678   SCAP.V.400.1: The vendor SHALL provide documentation and instruction on how to import
679   SCAP source data streams for the target platform.

680   **Required Test Procedures:**

681   SCAP.T.400.1: The tester SHALL import valid SCAP source data streams for the target platform
682   into the vendor product and execute the data streams on a target system. Results of the scan
683   SHALL be inspected to ensure actual results match expected results.

684   SCAP.T.400.2: The tester SHALL import an invalid SCAP source data stream into the vendor
685   product and ensure that the imported content is not available for execution.

686 **SCAP.R.500: The product SHALL be able to select a specific SCAP source data stream when**
687 **processing an SCAP data stream collection.**

688   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

689   **Required Vendor Information:**

690   SCAP.V.500.1: The vendor SHALL provide documentation and instruction on how to select a
691   specific data stream (by ID) when processing an SCAP data stream collection.

692   **Required Test Procedures:**

693   SCAP.T.500.1: The tester SHALL validate the vendor product can selectively choose and apply a
694   specific valid SCAP data stream.

695   **SCAP.R.600: The product SHALL be able to select a specific XCCDF benchmark within an SCAP**
696   **source data stream or data stream collection when multiple XCCDF benchmarks are present.**

697   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

698   **Required Vendor Information:**

699   SCAP.V.600.1: The vendor SHALL provide documentation and instruction on how to select a
700   specific XCCDF benchmark (by ID) when processing an SCAP data stream or data stream
701   collection.

702   **Required Test Procedures:**

703   SCAP.T.600.1: The tester SHALL validate the vendor product can selectively choose and apply a
704   specific valid XCCDF benchmark.

705   **SCAP.R.700: The product SHALL be able to select a specific XCCDF profile within an SCAP**
706   **source data stream or data stream collection when multiple XCCDF profiles are present.**

707   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

708   **Required Vendor Information:**

709   SCAP.V.700.1: The vendor SHALL provide documentation and instruction on how to select a
710   specific XCCDF profile (by ID) when processing an SCAP data stream or data stream collection.

711   **Required Test Procedures:**

712   SCAP.T.700.1: The tester SHALL validate the vendor product can selectively choose and apply a
713   specific valid XCCDF profile.

714   **SCAP.R.800: The product SHALL enable the user to import (signed and unsigned) SCAP source**
715   **data streams.**

716   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

717   **Required Vendor Information:**

718   SCAP.V.800.1: The vendor SHALL provide documentation explaining how an SCAP source data
719   stream can be imported into the product and subsequently executed.

720   **Required Test Procedures:**

721   SCAP.T.800.1: The tester SHALL verify that the product documentation includes instructions on
722   how the end user can import an SCAP source data stream.

723   SCAP.T.800.2: The tester SHALL import a valid unsigned SCAP source data stream into the
724   vendor product and ensure that the imported content is available for execution.

725   SCAP.T.800.3: The tester SHALL import a valid signed SCAP source data stream into the
726   vendor product and ensure that the imported content is available for execution.

727   **SCAP.R.900: The product SHALL recognize and reject SCAP source data streams that have**
728   **invalid signatures.**

729   This requirement has been deferred.

730   **SCAP.R.1000: The product SHALL recognize and reject SCAP source data streams that have**
731   **signatures based on invalid certificates.**

732   This requirement has been deferred.

733   **SCAP.R.1100: The product SHALL be able to correctly import all earlier versions of SCAP**
734   **content.**
735
736   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

737   **Required Vendor Information:**

738   SCAP.V.1100.1: The vendor SHALL provide documentation explaining how earlier versions of
739   SCAP content can be imported into the product and subsequently executed.

740   **Required Test Procedures:**

741   SCAP.T.1100.1: Using the vendor product, the tester SHALL execute a valid SCAP source data
742   stream based on SCAP 1.0 and SCAP 1.1 content.

743   **SCAP.R.1200: The product SHALL be able to determine the applicability of an imported SCAP**
744   **source data stream by evaluating the associated OVAL definition for the CPE Name on an XCCDF**
745   **<Benchmark>, <Profile>, <Group>, or <Rule> and verifying that the associated XCCDF content**
746   **applies to the target system.**

747   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

748   **Required Vendor Information:**

749   SCAP.V.1200.1: The vendor SHALL provide instructions on how the product indicates the
750   applicability of the imported SCAP source data stream to a target platform. Instructions
751   SHOULD also describe how the imported data stream is indicated to not be applicable for a target
752   platform. This requirement is testing the use of the OVAL check associated with a CPE name via
753   the CPE dictionary and platform id to determine applicability of the data stream.

754   **Required Test Procedures:**

755   SCAP.T.1200.1: The tester SHALL import an SCAP source data stream into the product that
756   contains a CPE Name and platform id and related OVAL definition not applicable for the target
757   system. The tester SHALL verify that the product declines to execute the non-applicable tests.

758   SCAP.T.1200.2: The tester SHALL import an SCAP source data stream into the product that
759   contains a CPE Name and platform id and related OVAL definition applicable for the target
760   system. The tester SHALL verify that the product executes the applicable tests.

761 **SCAP.R.1300: The product SHALL report and MAY reject OVAL content that is part of an SCAP**
762 **source data stream and that is invalid according to the OVAL XML schemas and Schematron style**
763 **sheets.[11]**

764   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

765   **Required Vendor Information:**

766   SCAP.V.1300.1: The vendor SHALL provide instructions on how validation of OVAL content
767   that is part of an SCAP data stream is performed and where errors from validation will be
768   displayed within the product output.

769   **Required Test Procedures:**

770   SCAP.T.1300.1: The tester SHALL attempt to import known invalid OVAL content that is part
771   of an SCAP data stream into the vendor product and examine the product output to validate that
772   the product reports the invalid OVAL content. The product MAY reject the content as invalid
773   according to the OVAL Definition schema and Schematron style sheets.

774 **SCAP.R.1400: The product SHALL report and MAY reject OCIL content that is invalid according**
775 **to the OCIL XML schema.**

776   **SCAP Capability:**   ☐ ACS   ☐ CVE   ☑ OCIL

777   **Required Vendor Information:**

778   SCAP.V.1400.1: The vendor SHALL provide instructions on how validation of OCIL content is
779   performed and where errors from validation will be displayed within the product output.

780   **Required Test Procedures:**

781   SCAP.T.1400.1: The tester SHALL attempt to import known invalid OCIL content into the
782   vendor product and examine the product output to validate that the product reports the invalid
783   OCIL content. The product MAY reject the content as invalid according to the OCIL XML
784   schema.

785 **SCAP.R.1500: The product SHALL be able to correctly assess the target systems using USGCB**
786 **source data streams as input.[12]**

787   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

788   **Required Vendor Information:**

---

[11]   This does not imply that the product being tested MUST use Schematron; the product needs only to produce the same results
as the Schematron implementation.
[12]   In the case where the Tier IV repository does not contain a source data stream for the tested platform, the tester SHALL use
a source data stream from Tier III. In case there is no content applicable to the tested platform, this requirement does not
apply.

789 SCAP.V.1500.1: The vendor SHALL provide instructions on how to import and execute valid
790 USGCB source data streams.

791 SCAP.V.1500.2: The lab or the vendor SHALL provide the scan results for each tested platform
792 using USGCB content associated with the platforms for which validation is being sought. The
793 tested systems SHALL be configured as Exact Compliance Configuration (the configuration
794 settings are equal to the discrete settings defined in the baseline).

795 **Required Test Procedures:**

796 Per vendor instruction in SCAP.V.1500.1, the lab or the vendor will configure the test systems,
797 make the necessary configuration changes to the target platform, and document what has been
798 changed. The pass/fail comparison of these changes SHALL NOT impact the Pass or Fail result
799 of the test.

800 All the applicable USGCB source data streams published in the official National Checklist
801 Program Repository should be used for testing this requirement: http://checklists.nist.gov.

802 SCAP.T.1500.1: The lab or the vendor SHALL evaluate the compliant target platforms, in a
803 domain connected configuration for Windows and standalone configuration for other platforms
804 (i.e., RHEL, Mac OS X, Unix, etc.), and compare the pass/fail results from the product to the
805 expected results, ensuring the actual results match the expected results. If the testing is performed
806 by the vendor, the source data streams, the scan results, and their hashes[13] will be submitted to the
807 lab for verification.

808 SCAP.T.1500.2: The tester SHALL review the scan results to ensure the files have not been
809 altered, the actual results match expected results, and pass the SCAPVal validation without any
810 errors.

811 **SCAP.R.1510: The product SHALL be able to correctly evaluate a patches up-to-date rule which**
812 **references an OVAL source data stream component consistent with the normative guidance**
813 **specified in [NIST SP 800-126 R2], against target systems of the target platform type and produce**
814 **the expected results.**

815 **SCAP Capability:** ☑ ACS ☐ CVE ☐ OCIL

816 **Required Vendor Information:**

817 SCAP.V.1510.1: The vendor SHALL provide instructions on how to import and execute a valid
818 SCAP source data stream with a patches up-to-date rule. The vendor SHALL also provide
819 instructions on where the resultant ARF XML Result output can be viewed by the tester.

820 **Required Test Procedures:**

821 Per vendor instruction in SCAP.V.1510, the tester SHALL evaluate the target platform(s) using
822 test content with patches up-to-date rule(s), validate results produced with SCAPVal, and
823 compare actual results to expected results, ensuring actual results match expected results.

824 SCAP.T.1510.1: The tester SHALL evaluate the target platform(s), in a domain connected
825 configuration for Windows and standalone configuration for other platforms, validate results

---

[13] The hashes SHALL comply with *Annex A: Approved Security Functions* of [FIPS 140-2].

826 produced with SCAPVal, and compare the scan results produced by the product to the expected
827 results, ensuring the actual results match the expected results.

828 **SCAP.R.1600: If the vendor product requires a specific configuration of the target platform that is**
829 **not in compliance with the USGCB checklist, the vendor SHALL provide documentation indicating**
830 **which settings require modification and a rationale for each changed setting. Products SHOULD**
831 **only require changes to the target platform if needed for product functionality.**

832 NOTE: Pursuant to the U.S. Office of Management and Budget (OMB) Memorandum M-08-22
833 to Federal CIOs: "Both industry and government information technology providers must use
834 SCAP validated tools with FDCC Scanner capability to certify their products operate correctly
835 with FDCC configurations and do not alter FDCC settings." [OMB M-08-22] Products
836 undergoing SCAP validations are required by OMB to make this self-assertion. Listing non-
837 complaint settings in no way negates the OMB M-08-22 requirement.

838 **SCAP Capability:** ☑ ACS ☐ CVE ☐ OCIL

839 **Required Vendor Information:**

840 SCAP.V.1600.1: The vendor SHALL provide an English language document to the lab that
841 indicates which settings require modification and a rationale for each changed setting. This
842 content will be used on NIST web pages to explain details about each validated product and thus
843 SHOULD contain only information that is to be publicly released.

844 **Required Test Procedures:**

845 SCAP.T.1600.1: The tester SHALL review the provided documentation to ensure that each
846 indicated setting includes an associated rationale.

847 **SCAP.R.1700: The product SHALL be able to correctly process the content that is representative**
848 **of content published at Tier III, Tier IV, and the OVAL repository[14] which is associated with the**
849 **platforms for which validation is being sought.**

850 **SCAP Capability:** ☑ ACS ☐ CVE ☐ OCIL

851 **Required Vendor Information:**

852 SCAP.V.1700.1: The vendor SHALL provide instructions on how to execute a previously
853 imported valid data stream for platforms supported.

854 **Required Test Procedures:**

855 SCAP.T.1700.1: Per vendor instruction in SCAP.V.1700, the tester SHALL evaluate a target
856 platform using test content representative of Tier III content, validate results produced with
857 SCAPVal, and ensure actual results match expected results.

858 **SCAP.R.1800: The product SHALL be able to determine the applicability of an imported SCAP**
859 **source data stream by evaluating the associated OCIL questionnaire for the CPE Name and**
860 **platform id on an XCCDF <Benchmark>, <Profile>, <Group>, or <Rule> and verifying that the**
861 **associated XCCDF content applies to the target system.**

---

[14] The OVAL repository is hosted by MITRE Corporation: https://oval.mitre.org/repository/.

862   **SCAP Capability:**   ☐ ACS   ☐ CVE   ☑ OCIL

863   **Required Vendor Information:**

864   SCAP.V.1800.1: The vendor SHALL provide instructions on how the product indicates the
865   applicability of the imported SCAP source data stream to a target platform. Instructions
866   SHOULD also describe how the product indicates data streams are not applicable for a target
867   platform. This requirement is testing the use of the OCIL questionnaire associated with a CPE
868   name via the CPE dictionary and the platform id to determine applicability of the data stream.

869   **Required Test Procedures:**

870   SCAP.T.1800.1: The tester SHALL import an SCAP source data stream into the product that
871   contains a CPE Name and related OCIL questionnaire not applicable for the target system. The
872   tester SHALL verify that the product declines to execute the non-applicable tests.

873   **SCAP.R.1900: The product SHALL be able to correctly evaluate a valid OVAL Definition file and**
874   **external variable file, where the contents of the OVAL Definition file are consistent with the**
875   **normative guidance[15] specified in [NIST SP 800-126 R1], against target systems of the target**
876   **platform type and produce a result file for each definition using the OVAL XML Full Results**
877   **expressed as Single Machine Without System Characteristics, Single Machine With System**
878   **Characteristics, and Single Machine With Thin Results.[16]**

879   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

880   **Required Vendor Information:**

881   SCAP.V.1900.1: The vendor SHALL provide instructions on how a valid OVAL Definitions file
882   and external variable file can be imported into the product for interpretation. The vendor SHALL
883   also provide instructions on where the resultant OVAL XML Results output can be viewed by the
884   tester.

885   **Required Test Procedure**

886   SCAP.T.1900.1: The tester SHALL run the product using valid OVAL Definitions files and an
887   external variable file against the test system of the target platform type. The actual results
888   SHALL match the expected results.

889   SCAP.T.1900.2: The tester SHALL validate the resulting OVAL XML Full Results by importing
890   the result set into the SCAPVal utility and checking for validation errors.

891   SCAP.T.1900.3: The tester SHALL validate that the resulting OVAL XML Full Results are
892   available for viewing by the user.

893   SCAP.T.1900.4: After the test system is assessed using the OVAL file, the tester SHALL capture
894   the successful results of the scan and verify the correctness of the results.

---

[15]   The supported OVAL tests are published at http://scap.nist.gov/validation/index.html.
[16]   The use case for OVAL-Only Scanning is described in Section 5.4 of [NIST SP 800-126 R1].

895   SCAP.T.1900.5: When the OVAL Definition file has been evaluated with the external variable
896   file that defines different values for the variables, the tester SHALL validate that the OVAL XML
897   Full Results file includes unique variable values as defined in the external variables file.

898   **SCAP.R.2000: The product SHALL be able to correctly evaluate a valid OVAL Definition file that**
899   **is part of an SCAP data stream, where the contents of the OVAL definition file are consistent with**
900   **the normative guidance[17] specified in [NIST SP 800-126 R2], against target systems of the target**
901   **platform type and produce a result file for each definition using the OVAL XML Full Results**
902   **expressed as Single Machine Without System Characteristics, Single Machine With System**
903   **Characteristics, and Single Machine With Thin Results.**

904   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

905   **Required Vendor Information:**

906   SCAP.V.2000.1: The vendor SHALL provide instructions on how a valid SCAP data stream file
907   can be imported into the product for interpretation. The vendor SHALL also provide instructions
908   on where the resultant SCAP Results output can be viewed by the tester.

909   **Required Test Procedure:**

910   SCAP.T.2000.1: The tester SHALL run the product using a valid SCAP data stream against the
911   target systems of the target platform type. The actual results SHALL match the expected results.

912   SCAP.T.2000.2: The tester SHALL validate the resulting SCAP data stream by importing it into
913   the SCAPVal utility and checking for any validation errors.

914   SCAP.T.2000.3: The tester SHALL validate that the resulting SCAP data stream is available for
915   viewing by the user.

916   SCAP.T.2000.4: The tester SHALL capture the successful results of the import and verify the
917   correctness of the results.

918   **SCAP.R.2100: The product SHALL be able to correctly evaluate a valid OCIL Questionnaire file**
919   **against test systems of the target platform type, and produce a valid OCIL Output file (i.e., file that**
920   **includes both the original content and the evaluation results) using the format defined by the OCIL**
921   **XML schema.**

922   **SCAP Capability:**   ☐ ACS   ☐ CVE   ☑ OCIL

923   **Required Vendor Information:**

924   SCAP.V.2100.1: The vendor SHALL provide instructions on how a valid OCIL Questionnaire
925   file can be imported into the product for interpretation. The vendor SHALL also provide
926   instructions on where the resultant OCIL Output file can be viewed by the tester.

927   **Required Test Procedure:**

---

[17]   The supported OVAL tests are published at http://scap.nist.gov/validation/index.html.

928   SCAP.T.2100.1: The tester SHALL run the product using valid OCIL document files against the
929   test systems of the target platform type. The results SHALL be verified by the tester, ensuring
930   each OCIL definition and criteria contained within the definition produces the correct response.

931   SCAP.T.2100.2: The tester SHALL validate the resulting OCIL Output file with the SCAPVal
932   utility and check for any validation errors.

933   SCAP.T.2100.3: The tester SHALL validate that the resulting OCIL Output file is available for
934   viewing by the user.

935   **SCAP.R.2200: The product SHALL be able to correctly evaluate a valid OCIL Questionnaire file**
936   **that is part of an SCAP source data stream against target systems of the target platform type, and**
937   **produce a valid OCIL Output file (i.e., file that includes both the original content and the**
938   **evaluation results) using the format defined by the OCIL XML schema.**

939   **SCAP Capability:**   ☐ ACS   ☐ CVE   ☑ OCIL

940   **Required Vendor Information:**

941   SCAP.V.2200.1: The vendor SHALL provide instructions on how a valid OCIL Questionnaire
942   file that is part of an SCAP source data stream can be imported into the product for interpretation.
943   The vendor SHALL also provide instructions on where the resultant SCAP data stream can be
944   viewed by the tester.

945   **Required Test Procedure:**

946   SCAP.T.2200.1: The tester SHALL run the product using valid SCAP data stream files against
947   the target systems of the target platform type. The actual results SHALL match the expected
948   results.

949   SCAP.T.2200.2: The tester SHALL validate the resulting SCAP data stream by importing it into
950   the SCAPVal utility and checking for any validation errors.

951   SCAP.T.2200.3: The tester SHALL validate that the resulting SCAP data stream is available for
952   viewing by the user.

953   **SCAP.R.2300: The product SHALL indicate the correct CCE ID for each configuration issue**
954   **referenced within the product that has an associated CCE ID (i.e., the product's CCE mapping**
955   **MUST be correct).**

956   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

957   **Required Vendor Information:**

958   SCAP.V.2300.1: None.

959   **Required Test Procedures:**

960   SCAP.T.2300.1: Using the product output from SCAP.R.2930, the tester SHALL compare the
961   vendor data against the official CCE description. The tester SHALL perform the comparison
962   using a non-vendor-directed sample comprised of greater than or equal to 10 and less than or
963   equal to 30 of the total configuration issue items with CCE IDs. The tester SHOULD prove that

964   the vendor's CCE ID correctly maps to the configuration issue. This test ensures that the product
965   correctly maps to CCE IDs, but does not test for completeness of the mapping.

966 **SCAP.R.2400: The product SHALL associate an existing CCE ID to each configuration issue**
967 **referenced within the product for which a CCE ID exists (i.e., the product's CCE mapping MUST**
968 **be complete).**

969   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

970   **Required Vendor Information:**

971   SCAP.V.2400.1: None.

972   **Required Test Procedures:**

973   SCAP.T.2400.1: Using the list of configuration issue items produced in SCAP.R.2930, the tester
974   SHALL examine the descriptions and search the CCE dictionary for all corresponding CCE IDs.
975   The tester SHALL perform this using a non-vendor-directed sample comprised of 10 % of the
976   total configuration issue items with no CCE IDs, up to a maximum of 30. The tester does not
977   need to rigorously prove that no CCE ID exists, only that there does not appear to be a match.
978   This test ensures that the product has a complete mapping to CCE, but does not test the
979   correctness of the mapped data.

980 **SCAP.R.2500: If the product natively contains a product dictionary (as opposed to dynamically**
981 **importing content containing CPE names), the product MUST contain CPE naming data from the**
982 **current official CPE Dictionary.**

983   **NOTE:** This requirement does not apply if the product is using the official dynamic CPE
984   Dictionary as provided on the NVD web site or as part of an SCAP source data stream.

985   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

986   **Required Vendor Information:**

987   SCAP.V.2500.1: The vendor SHALL provide a list of all CPE names included in the product
988   using the standard CPE Dictionary XML schema as provided in the CPE Specification version
989   cited in Section 2.5.

990   SCAP.V.2500.2: If the vendor product includes CPE names that are not in the official CPE
991   Dictionary, a listing of exceptions MUST be provided.

992   **Required Test Procedures:**

993   SCAP.T.2500.1: The tester SHALL compare the vendor-provided list of CPE Names against the
994   official CPE Dictionary.[18] The tester SHALL verify that all exceptions found match the list of
995   exceptions provided by the vendor.

996 **SCAP.R.2600: Products MUST process CPEs referenced in an *<xccdf:platform>* element directly or**
997 **by a *<cpe2:fact-ref>* contained within a referenced *<cpe2:platform-specification>* element as**
998 **specified in [NIST SP 800-126 R2].**

---

[18]   http://static.nvd.nist.gov/feeds/xml/cpe/dictionary/official-cpe-dictionary_v2.2.xml

999

1000   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1001   **Required Vendor Information:**

1002   SCAP.V.2600.1**:** The vendor SHALL provide instructions describing how to import an SCAP
1003   source data stream that contains references to CPEs in an *<xccdf:platform>* element directly or by
1004   a *<cpe2:fact-ref>* contained within a referenced *<cpe2:platform-specification>* element and have
1005   it applied against a known platform. The vendor SHALL also provide instructions on how to
1006   view the results of the application of the content against the platform.

1007   **Required Test Procedures:**

1008   SCAP.T.2600.1: The tester SHALL import the known content into the product and apply it
1009   against a known platform.
1010
1011   SCAP.T.2600.2: The tester SHALL import the results of the content into the SCAPVal utility and
1012   check for any validation errors.
1013
1014   SCAP.T.2600.3: The tester SHALL ensure the actual results match the expected results.
1015
1016   **SCAP.R.2700: The product SHALL indicate the correct CVE ID or metadata for each software**
1017   **flaw and/or patch definition referenced within the product that has an associated CVE ID (i.e., the**
1018   **product's CVE mapping MUST be correct).**

1019   **SCAP Capability:**   ☐ ACS   ☑ CVE   ☐ OCIL

1020   **Required Vendor Information:**

1021   SCAP.V.2700.1: None

1022   **Required Test Procedures:**

1023   SCAP.T.2700.1: Using the product output from SCAP.R.2920, the tester SHALL compare the
1024   vendor data against the official NVD CVE ID description and references. The tester SHALL
1025   perform this test using a non-vendor-directed sample comprised of 10 % of the total software
1026   flaws and/or patches with CVE IDs, up to a maximum of 30. The tester does not need to
1027   rigorously prove that the vendor's software flaw and/or patch description matches the NVD CVE
1028   description, but merely needs to identify that the two descriptions appear to pertain to the same
1029   vulnerability. This test ensures that the product correctly maps to CVE, but does not test for
1030   completeness of the mapping.

1031   It is sufficient to provide URLs that link to the NVD website. For example,
1032   http://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2011-1377. It is not sufficient to provide a
1033   URL to http://web.nvd.nist.gov.

1034   **SCAP.R.2800: The product SHALL associate an existing CVE ID to each software flaw and/or**
1035   **patch referenced within the product for which a CVE ID exists (i.e., the product's CVE mapping**
1036   **MUST be complete).**

1037   **SCAP Capability:**   ☐ ACS   ☑ CVE   ☐ OCIL

1038   **Required Vendor Information:**

1039   SCAP.V.2800.1: None.

1040   **Required Test Procedures:**

1041   SCAP.T.2800.1: Using the list of software flaws produced in SCAP.R.2920, the tester SHALL
1042   examine the descriptions and search the NVD for any corresponding CVE IDs. The tester
1043   SHALL perform this using a non-vendor-directed sample comprised of 10 % of the total software
1044   flaws and/or patches with no CVE IDs, up to a maximum of 30. The tester does not need to
1045   rigorously prove that no CVE ID exists, only that there does not appear to be a match. This test
1046   ensures that the product has a complete mapping to CVE, but does not test the correctness of the
1047   mapped data.

1048   **4.3   SCAP Result(s) Data Stream**

1049   This section addresses those requirements that assess a product's ability to produce validated SCAP
1050   results.

1051   **SCAP.R.2900: SCAP result data streams SHALL be produced by the product in compliance with**
1052   **the SCAP result data streams as specified in [NIST SP 800-126 R2].**

1053   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1054   **Required Vendor Information:**

1055   SCAP.V.2900.1: The vendor SHALL provide instruction on where the corresponding XCCDF
1056   and OVAL results files can be located for inspection.

1057   **Required Test Procedures:**

1058   SCAP.T.2900.1: The tester SHALL visually inspect SCAP results to verify that they are valid
1059   according to the associated specification for each. The SCAP output MUST be processed by the
1060   SCAPVal utility without any errors.

1061   **SCAP.R.2910: The product SHALL be able to correctly import and evaluate SCAP source data**
1062   **streams which reference external content consistent with the normative guidance specified in NIST**
1063   **[NIST SP 800-126 R2], against target systems of the target platform type and produce the expected**
1064   **results.**

1065   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1066   **Required Vendor Information:**

1067   SCAP.V.2910.1: The vendor SHALL provide instructions on how to import and execute a valid
1068   SCAP source data stream with references to external content. The vendor SHALL also provide
1069   instructions on where the resultant ARF XML Result output can be viewed by the tester.

1070   **Required Test Procedures:**

1071   Per vendor instruction in SCAP.V.2910, the tester SHALL evaluate the target platform(s) using
1072   test content with references to external content, validate results produced with SCAPVal, and
1073   compare actual results to expected results, ensuring actual results match expected results.

1074   SCAP.T.2910.1: The tester SHALL evaluate the target platform(s), in a domain connected
1075   configuration for Windows and standalone configuration for other platforms, validate results
1076   produced with SCAPVal, and compare the scan results produced by the product to the expected
1077   results, ensuring the actual results match the expected results.

1078   **SCAP.R.2920: The product SHALL be able to assign CVE identifiers to rule results in compliance**
1079   **with the SCAP result data streams as specified in [NIST SP 800-126 R2].**

1080   **SCAP Capability:**   ☑ ACS   ☑ CVE   ☐ OCIL

1081   **Required Vendor Information:**

1082   SCAP.V.2920.1: The vendor SHALL provide instruction on where the SCAP Result Data
1083   Stream files can be located for inspection.

1084   **Required Test Procedures:**

1085   SCAP.T.2920.1: The tester SHALL visually inspect the results to verify that the CVE identifiers
1086   are included within the <xccdf:rule-result> element. The SCAP Result Data Streams MUST be
1087   processed by the SCAPVal utility without any errors.

1088   **SCAP.R.2930: The product SHALL be able to assign CCE identifiers to rule results in compliance**
1089   **with the SCAP result data streams as specified in [NIST SP 800-126 R2].**

1090   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1091   **Required Vendor Information:**

1092   SCAP.V.2930.1: The vendor SHALL provide instruction on where the SCAP Result Data
1093   Stream files can be located for inspection.

1094   **Required Test Procedures:**

1095   SCAP.T.2930.1: The tester SHALL visually inspect the results to verify that the CCE identifiers
1096   are included within the <xccdf:rule-result> element. The SCAP Result Data Streams MUST be
1097   processed by the SCAPVal utility without any errors.

1098   **SCAP.R.2940: The product SHALL be able to assign CPE identifiers to rule results in compliance**
1099   **with the SCAP result data streams as specified in [NIST SP 800-126 R2].**

1100   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1101   **Required Vendor Information:**

1102   SCAP.V.2940.1: The vendor SHALL provide instruction on where the SCAP Result Data
1103   Stream files can be located for inspection.

1104   **Required Test Procedures:**

1105   SCAP.T.2940.1: The tester SHALL visually inspect the results to verify that the CPE identifiers
1106   are included within the <xccdf:rule-result> element. The SCAP Result Data Streams MUST be
1107   processed by the SCAPVal utility without any errors.

1108   **SCAP.R.3000: The product SHALL be able to process XCCDF components that are part of an**
1109   **SCAP source data stream and generate XCCDF component results within an SCAP result data**
1110   **stream in accordance with the XCCDF specification for the target platform.[19]**

1111   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1112   **NOTE:** "XCCDF components" refer to the elements such as benchmark, profile, group, rule,
1113   value, and test result.

1114   **Required Vendor Information:**

1115   SCAP.V.3000.1: The vendor SHALL provide instructions on how to import XCCDF component
1116   content that is part of SCAP source data streams for execution and provide instructions on where
1117   the XCCDF component results can be located for visual inspection. The purpose of this
1118   requirement is to ensure that the product produces valid XCCDF Results and a matching "pass"/
1119   "fail" result for a given rule.

1120   **Required Test Procedures:**

1121   SCAP.T.3000.1: The tester SHALL import a known valid XCCDF component content that is part
1122   of SCAP data streams for the target platform into the vendor product and execute it according to
1123   the product operation instructions provided by the vendor. The tester will inspect the product
1124   output ensuring XCCDF components are compliant with the XCCDF specification.

1125   SCAP.T.3000.2: The tester SHALL validate the resulting XCCDF component results within an
1126   SCAP result data stream output using the SCAPVal utility. This validation MUST NOT produce
1127   any validation errors.

1128   SCAP.T.3000.3: The tester SHALL compare the product results to the expected results ensuring
1129   that the "pass"/ "fail" results match for each Rule.

1130
1131   **SCAP.R.3005: The product SHALL be able to process XCCDF Tailoring component**
1132   **(<xccdf:Tailoring>) that is part of an SCAP source data stream as well as XCCDF Tailoring**
1133   **component that is external to the source datastream and generate XCCDF component results**
1134   **within an SCAP result data stream in accordance with the XCCDF specification for the target**
1135   **platform.**

1136   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1137   **Required Vendor Information:**

1138   SCAP.V.3005.1: The vendor SHALL provide instructions on how to import XCCDF Tailoring
1139   component content that is part of or external to the SCAP source data streams for execution and
1140   provide instructions on where the XCCDF component results can be located for visual inspection.

---

[19] XCCDF Specification in [NISTIR 7275 R4].

1141 The purpose of this requirement is to ensure that the product produces valid XCCDF Results and
1142 the results match the expected results for all given rules.

1143 **Required Test Procedures:**

1144 SCAP.T.3005.1: The tester SHALL import a known valid XCCDF Tailoring component content
1145 that is part of SCAP source data streams for the target platform into the vendor product and
1146 execute it according to the product operation instructions provided by the vendor. The tester will
1147 inspect the product output ensuring XCCDF components are compliant with the XCCDF
1148 specification.

1149 SCAP.T.3005.2: The tester SHALL import a known valid XCCDF Tailoring component content
1150 that is external to the SCAP source data streams for the target platform into the vendor product
1151 and execute it according to the product operation instructions provided by the vendor. The tester
1152 will inspect the product output ensuring XCCDF components are compliant with the XCCDF
1153 specification.

1154 SCAP.T.3005.3: The tester SHALL validate the resulting XCCDF component results within an
1155 SCAP result data stream output using the SCAPVal utility. This validation MUST NOT produce
1156 any validation errors.

1157 SCAP.T.3005.4: The tester SHALL compare the product results to the expected results ensuring
1158 that all the results match the expected results.

1159

1160 **SCAP.R.3010: The product SHALL be able to select and process XCCDF Benchmark components,**
1161 **which do not include <xccdf:Profile> elements, that are part of an SCAP source data stream and**
1162 **generate XCCDF component results within an SCAP result data stream in accordance with the**
1163 **XCCDF specification for the target platform.**

1164 **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1165 **Required Vendor Information:**

1166 SCAP.V.3010.1: The vendor SHALL provide instructions on how to import XCCDF component
1167 content without <xccdf:Profile> elements that is part of SCAP source data streams for execution
1168 and provide instructions on where the XCCDF component results can be located for visual
1169 inspection. The purpose of this requirement is to ensure that the product produces valid XCCDF
1170 Results and the results match the expected results for all given rules.

1171 **Required Test Procedures:**

1172 SCAP.T.3010.1: The tester SHALL import a known valid XCCDF component content without
1173 <xccdf:Profile> elements that is part of SCAP data streams for the target platform into the vendor
1174 product and execute it according to the product operation instructions provided by the vendor.
1175 The tester will inspect the product output ensuring XCCDF components are compliant with the
1176 XCCDF specification.

1177   SCAP.T.3010.2: The tester SHALL validate the resulting XCCDF component results within an
1178   SCAP result data stream output using the SCAPVal utility. This validation MUST NOT produce
1179   any validation errors.

1180   SCAP.T.3010.3: The tester SHALL compare the product results to the expected results ensuring
1181   that all the results match the expected results.

1182   **SCAP.R.3100: For all CCE IDs in the SCAP source data stream, the product SHALL correctly**
1183   **display the CCE ID with its associated XCCDF Rule in the product output.**

1184   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1185   **Required Vendor Information:**

1186   SCAP.V.3100.1: The vendor SHALL provide instructions on where the XCCDF Rules and their
1187   associated CCE IDs can be visually inspected within the product output.

1188   **Required Test Procedures:**

1189   SCAP.T.3100.1: The tester SHALL visually inspect a non-vendor-directed sample of 10 % of the
1190   XCCDF Rules, up to a maximum of 30, within the product output and reports to validate that the
1191   CCE IDs for each inspected XCCDF Rule match those found in the XCCDF source file.

1192   **SCAP.R.3200: The product output SHALL enable users to view the XML OCIL Questionnaires**
1193   **being consumed by the product (e.g., within the product user interface or through an XML dump**
1194   **of the OCIL questionnaires to a file).**

1195   **SCAP Capability:**   ☐ ACS   ☐ CVE   ☑ OCIL

1196   **Required Vendor Information:**

1197   SCAP.V.3200.1: The vendor SHALL provide instructions on how the user can view the XML
1198   OCIL Questionnaires being consumed by the product.

1199   **Required Test Procedure:**

1200   SCAP.T.3200.1: The tester SHALL follow the provided vendor instructions to view the XML
1201   OCIL Questionnaires being consumed by the product and verify that access is provided as stated.

1202   **SCAP.R.3300: The product SHALL be able to produce "notchecked" results for unsupported**
1203   **Check Systems. [20]**

1204   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1205   **Required Vendor Information:**

1206   SCAP.V.3300.1: The vendor SHALL provide instructions indicating how content for
1207   unsupported check systems is processed.

1208   **Required Test Procedures:**

---

[20] XCCDF Specification in [NISTIR 7275 R4].

1209   SCAP.T.3300.1: The tester SHALL import a valid SCAP source data stream containing a check
1210   system unsupported by the vendor product for the target platform into the product and execute the
1211   data stream according to the product operation instructions provided by the vendor. The tester
1212   SHALL inspect the product output to validate that it includes "notchecked" results for the
1213   unsupported check system.

1214 **SCAP.R.3400: The product output SHALL enable users to view the XML OVAL Definitions being**
1215 **consumed by the product (e.g., within the product user interface or through an XML dump of the**
1216 **OVAL definitions to a file).**

1217   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1218   **Required Vendor Information:**

1219   SCAP.V.3400.1: The vendor SHALL provide instructions on how the user can view the XML
1220   OVAL Definitions being consumed by the product.

1221   **Required Test Procedure:**

1222   SCAP.T.3400.1: The tester SHALL follow the provided vendor instructions to view the XML
1223   OVAL Definitions being consumed by the product and verify that access is provided as stated.

1224 **SCAP.R.3500: For all SCAP source data streams, the product SHALL indicate the date the data**
1225 **was last generated and updated. The generated date is when the data was originally**
1226 **created/officially published. The updated date is the date the product obtained its copy of the data.**

1227   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1228   **Required Vendor Information:**

1229   SCAP.V.3500.1: The vendor SHALL provide instructions on where the dates for all imported
1230   SCAP source data streams can be inspected in the product output.

1231   **Required Test Procedures:**

1232   SCAP.T.3500.1: The tester SHALL visually inspect the product output for the dates of all SCAP
1233   source data streams processed by the vendor product.

1234 **SCAP.R.3600: The product SHALL display the associated CCE ID for each configuration issue**
1235 **definition in the product output (i.e., the product displays CCE IDs).**

1236   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1237   **Required Vendor Information:**

1238   SCAP.V.3600.1: The vendor SHALL provide instructions on how product output can be
1239   generated that contains a listing of all security configuration issue items, with associated CCE IDs
1240   when available. Instructions SHALL include where the CCE IDs and the associated vendor
1241   supplied and/or official CCE descriptions can be located within the product output.

1242   **Required Test Procedures:**

1243   SCAP.T.3600.1: The tester SHALL visually inspect, within the product output, a non-vendor-
1244   directed set of 30 security configuration issue items, to ensure that the CCE IDs are displayed.
1245   This test is not intended to determine whether the product correctly maps to CCE or whether it
1246   provides a complete mapping.

1247   **SCAP.R.3700 has been removed.**

1248   **SCAP.R.3800: A product's machine-readable output MUST provide the CPE naming data using**
1249   **CPE names.**

1250   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1251   **Required Vendor Information:**

1252   SCAP.V.3800.1: The vendor SHALL provide procedures and/or a test environment where
1253   machine-readable output containing the CPE naming data can be produced and inspected. The
1254   vendor SHALL provide a translation tool to create human-readable data for inspection if the
1255   provided output is not in a human-readable format (e.g., binary data, encrypted text).

1256   **Required Test Procedures:**

1257   SCAP.T.3800.1: The tester SHALL manually inspect the vendor-identified machine-readable
1258   output and ensure that CPE naming data is correct according to the CPE specification. The tester
1259   will do this by choosing a minimum of 30 vendor and product names in the product output that
1260   are also included in the official CPE Dictionary.

1261   **SCAP.R.3900: The product SHALL allow users to locate configuration issue items using CCE IDs.**

1262   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1263   **Required Vendor Information:**

1264   SCAP.V.3900.1: The vendor SHALL provide documentation (printed or electronic) indicating
1265   how configuration issue items can be located using CCE IDs.

1266   **Required Test Procedures:**

1267   SCAP.T.3900.1: The tester SHALL verify that configuration issue items can be identified using
1268   CCE IDs. The tester SHALL perform this using a non-vendor-directed sample comprised of
1269   10 % of the total configuration issue items, up to a maximum of 30.

1270   **SCAP.R.4000: The product SHALL be able to correctly produce the Asset Identification Fields as**
1271   **specified in [NIST SP 800-126 R2] when assessing a target.**

1272   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1273   **Required Vendor Information:**

1274   SCAP.V.4000.1: The vendor SHALL provide documentation on how to import an SCAP data
1275   stream and how to apply it to a target system.

1276   **Required Test Procedures:**

1277   SCAP.T.4000.1: The tester SHALL import the SCAP source data stream and apply it to a known
1278   target, producing an SCAP result data stream.

1279   SCAP.T.4000.2: The tester SHALL validate the results produced using SCAPVal; the validation
1280   MUST NOT produce any errors.

1281   SCAP.T.4000.3: The tester SHALL visually inspect the results to ensure the Asset Identification
1282   Fields are as expected.

1283 **SCAP.R.4100: The product SHALL be able to correctly produce an SCAP result data stream**
1284 **conforming to the ARF specification for each XCCDF, OVAL, and OCIL component.**

1285   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☑ OCIL

1286   **Required Vendor Information:**

1287   SCAP.V.4100.1: The vendor SHALL supply documentation on how to import an SCAP data
1288   stream, apply it against a target, and produce an SCAP result data stream conforming to the ARF
1289   specification.

1290   **Required Test Procedures:**

1291   SCAP.T.4100.1: The tester SHALL import the SCAP 1.2 source data stream, apply it to a known
1292   target, and produce an SCAP result data stream conforming to the ARF specification.

1293   SCAP.T.4100.2: The tester SHALL validate the results produced using SCAPVal; the validation
1294   MUST NOT produce any errors.

1295   SCAP.T.4100.3: The tester SHALL compare the actual results to the expected results ensuring
1296   the results match.

1297 **SCAP.R.4200: The product SHALL provide a means to view the CVE Description and CVE**
1298 **references for each displayed CVE ID[21] within the product output.**

1299   **SCAP Capability:**   ☐ ACS   ☑ CVE   ☐ OCIL

1300   **Required Vendor Information:**

1301   SCAP.V.4200.1: The vendor SHALL provide instructions on where the CVE IDs can be located
1302   within the product output. The vendor SHALL provide procedures and a test environment (if
1303   necessary) so that the product will output vulnerabilities with associated CVE IDs. Instructions
1304   SHALL include where the CVE IDs and the associated vendor-supplied and official CVE
1305   descriptions can be located within the product output. It is acceptable to have CVEs in the form
1306   of a specific link for each CVE to the NVD.

1307   **Required Test Procedures:**

1308   SCAP.T.4200.1: The tester SHALL select a non-vendor-directed sampling of CVE IDs from
1309   within the available forms of the product output. The tester SHALL determine that the product

---

[21]   This requirement can be met by providing a URL to the NVD CVE or MITRE CVE vulnerability summaries for the CVE
        IDs in question.

1310   output enables the user to view, at minimum, the official CVE description and references.[22] The
1311   vendor MAY provide additional CVE descriptions and information. The tester SHALL perform
1312   this using a non-vendor-directed sample comprised of greater than or equal to 10 and less than or
1313   equal to 30 of the total CVE IDs available in the product output.

1314   **SCAP.R.4300: For all static or product -bundled CCE data, the product SHALL indicate the date**
1315   **the data was last generated and updated. The generated date is when the data was originally**
1316   **created/officially published. The updated date is the date the product obtained its copy of the data.**

1317   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1318   **Required Vendor Information:**

1319   SCAP.V.4300.1: The vendor SHALL provide instructions on where the dates for all offline CCE
1320   data can be inspected in the product output.

1321   **Required Test Procedures:**

1322   SCAP.T.4300.1: The tester SHALL visually inspect the product output for the dates of all static
1323   or bundled CCE data included with the vendor product.

1324   **SCAP.R.4400: The product SHALL include the CVE ID(s) associated with each software flaw**
1325   **and/or patch definition in the product output (i.e., the product displays CVE IDs) where**
1326   **appropriate.[23]**

1327   **SCAP Capability:**   ☐ ACS   ☑ CVE   ☐ OCIL

1328   **Required Vendor Information:**

1329   SCAP.V.4400.1: The vendor SHALL provide instructions, and a test environment (if necessary),
1330   indicating how product output can be generated that contains a listing of all software flaws and
1331   patches with associated CVE IDs when available. CVE IDs SHOULD be used wherever possible.
1332   Instructions SHALL include where the CVE IDs and the associated vendor-supplied and/or
1333   official CVE descriptions can be located within the product output.

1334   **Required Test Procedures:**

1335   SCAP.T.4400.1: The tester SHALL visually inspect, within the product output, a non-vendor-
1336   selected sample comprised of greater than or equal to 10 and less than or equal to 30 of the total
1337   CVE IDs available in the product output to ensure that the CVE IDs are displayed. This test is
1338   not intended to determine whether the product correctly maps to CVE or whether it provides a
1339   complete mapping.

1340   **SCAP.R.4500: If the product uses CVE, it SHALL include NVD CVSS base scores and vector**
1341   **strings for each CVE ID referenced in the product.**

1342   **SCAP Capability:**   ☐ ACS   ☑ CVE   ☐ OCIL

---

[22]   The official CVE description and references are found at http://nvd.nist.gov/.
[23]   In the case where the content being processed only requires results that do not contain CVE references this requirement does
       not apply.

1343   **Required Vendor Information:**

1344   SCAP.V.4500.1: The vendor SHALL provide documentation explaining where the NVD CVSS
1345   base scores and vector strings can be located with the corresponding CVE ID.[24] The vendor
1346   MAY provide information about how the product can be updated with new NVD CVSS base
1347   scores and vector strings prior to testing.

1348   **Required Test Procedure:**

1349   SCAP.T.4500.1: The tester SHALL update the product's NVD base scores and vectors (using the
1350   vendor-provided update capability if it exists) and validate that the product displays the NVD
1351   CVSS base scores and vectors for 15 non-vendor-directed CVE IDs referenced in the product.
1352   The CVEs chosen MUST have an NVD vulnerability summary "last revision" date that is at least
1353   30 days old. A link to the information on the NVD web site is sufficient for this test.

1354 **SCAP.R.4600: When processing SCAP source data streams that contain compliance mappings to**
1355 **CCEs, the product SHALL output the compliance mappings.[25]**

1356   **SCAP Capability:**   ☑ ACS   ☐ CVE   ☐ OCIL

1357   **Required Vendor Information:**

1358   SCAP.V.4600.1: The vendor SHALL provide documentation explaining where CCE to NIST SP
1359   800-53 compliance mappings can be viewed within the product output.

1360   **Required Test Procedures:**

1361   SCAP.T.4600.1: Using the vendor product, the tester SHALL execute a valid SCAP source data
1362   stream with CCE to NIST SP 800-53 compliance mapping information and view the resultant
1363   output to ensure that the CCE compliance mappings are correct.

1364

1365

---

[24]   A link to the specific CVE entry on the NVD web site is sufficient for this test.
[25]   The USGCB data streams have associated machine readable CCE to 800-53 mappings available at https://usgcb.nist.gov .

1366 **5.   Derived Test Requirements for Specific Capabilities**

1367 This section contains Derived Test Requirements for each of the defined SCAP capabilities. When a
1368 product is submitted for validation, the submitting organization will provide a list of SCAP capabilities
1369 the product possesses. The information regarding capabilities will be provided by the vendor as part of
1370 their submission package. To determine the correct test requirements for that product, the tester creates
1371 the union of all these capabilities using the chart below.

1372 The matrix currently contains a total of three SCAP capabilities. As additional capabilities are available
1373 for validation, this list will be updated. Vendors seeking validation for an SCAP capability not listed
1374 should contact NIST at scap@nist.gov.

1375 The following chart summarizes the requirements for each SCAP 1.2 capability.

1376   **Table 5-1. Required SCAP Components for Each SCAP Capability**

Requirement ID	Authenticated Configuration Scanner (ACS)	CVE option	OCIL option
SCAP.R.100	X		
SCAP.R.200	X		
SCAP.R.300	X		
SCAP.R.400	X		
SCAP.R.500	X		
SCAP.R.600	X		
SCAP.R.700	X		
SCAP.R.800	X		
SCAP.R.1100	X		
SCAP.R.1200	X		
SCAP.R.1300	X		
SCAP.R.1400			X
SCAP.R.1500	X		
SCAP.R.1510	X		
SCAP.R.1600	X		
SCAP.R.1700	X		
SCAP.R.1800			X
SCAP.R.1900	X		
SCAP.R.2000	X		
SCAP.R.2100			X
SCAP.R.2200			X

Requirement ID	Authenticated Configuration Scanner (ACS)	CVE option	OCIL option
SCAP.R.2300	X		
SCAP.R.2400	X		
SCAP.R.2500	X		
SCAP.R.2600	X		
SCAP.R.2700		X	
SCAP.R.2800		X	
SCAP.R.2900	X		
SCAP.R.2910	X		
SCAP.R.2920	X	X	
SCAP.R.2930	X		
SCAP.R.2940	X		
SCAP.R.3000	X		
SCAP.R.3005	X		
SCAP.R.3010	X		
SCAP.R.3100	X		
SCAP.R.3200			X
SCAP.R.3300	X		
SCAP.R.3400	X		
SCAP.R.3500	X		
SCAP.R.3600	X		
SCAP.R.3800	X		
SCAP.R.3900	X		
SCAP.R.4000	X		
SCAP.R.4100	X		X
SCAP.R.4200		X	
SCAP.R.4300	X		
SCAP.R.4400		X	
SCAP.R.4500		X	
SCAP.R.4600	X		

1377
1378
1379   CVE and OCIL are optional SCAP component specifications that may be combined with ACS in
1380   SCAP 1.2 product validations. Product vendors may elect adding CVE, OCIL, or both options to
1381   the core ACS product validation. If the CVE option is chosen, the product must pass all CVE

1382   requirements marked in the CVE column in Table 5-1. If the OCIL option is chosen, the product
1383   must pass all OCIL requirements marked in the OCIL column in Table 5-1. Products may not be
1384   validated against the CVE or OCIL requirements alone. These optional validations must be
1385   combined with the core ACS product validation.
1386
1387   **NOTE**: The ACS capability encompasses the functionality covered by FDCC Scanner and
1388   USGCB Scanner capabilities that were included in the SCAP 1.0 Validation Program.
1389
1390   The list of OVAL tests used for testing the ACS SCAP 1.2 capability is published on the SCAP
1391   Validation Program web page http://scap.nist.gov/validation.[26]
1392
1393

---

[26]   Support of deprecated OVAL tests is required for the Authenticated Configuration Scanner (ACS) capability. Backward
       compatibility is required for SCAP 1.2 validated products.

Appendix A—Terms and Definitions

This appendix lists definitions of key terms used in this document.

Authenticated Configuration Scanner: A product that runs with administrative or root privileges on a target system to conduct its assessment.

CCE ID: An identifier for a specific configuration defined within the official CCE Dictionary and that conforms to the CCE specification. For more information please see the CCE specification reference in Section 2.

Compliance Mapping: The process of correlating CCE settings defined in a source data stream with the security control identifiers defined in NIST SP 800-53.

CPE Name: An identifier for a unique uniform resource identifier (URI) assigned to a specific platform type that conforms to the CPE specification. For more information please see the CPE specification reference in Section 2.

CVE ID: An identifier for a specific software flaw defined within the official CVE Dictionary and that conforms to the CVE specification. For more information please see the CVE specification reference in Section 2.

Derived Test Requirement/Test Requirement: A statement of requirement, needed information, and associated test procedures necessary to test a specific SCAP feature.

Import: A process available to end users by which an SCAP source data stream can be loaded into the vendor's product. During this process, the vendor process may optionally translate this file into a proprietary format.

Machine-Readable: Product output that is in a structured format, typically XML, which can be consumed by another program using consistent processing logic.

Major Revision: Any increase in the version of an SCAP component's specification or SCAP related data set that involves substantive changes that will break backwards compatibility with previous releases. See also SCAP revision.

Minor Revision: Any increase in the version of an SCAP component's specification or SCAP related data set that may involve adding additional functionality, but that preserves backwards compatibility with previous releases. See also SCAP revision.

Misconfiguration: A setting within a computer program that violates a configuration policy or that permits or causes unintended behavior that impacts the security posture of a system. CCE can be used for enumerating misconfigurations.

> **NOTE:** NIST generally defines vulnerability as including both software flaws and configuration issues [misconfigurations]. For the purposes of the validation program and dependent procurement language, the SCAP Validation program is defining vulnerability and misconfiguration as two separate entities, with "vulnerability" referring strictly to software flaws.)

1430   **National Checklist Program Repository (NCP):** A NIST maintained repository, which is a publicly
1431   available resource that contains information on a variety of security configuration checklists for specific
1432   IT products or categories of IT products.
1433
1434   **National Vulnerability Database (NVD):** The U.S. government repository of standards based
1435   vulnerability management data represented using the Security Content Automation Protocol (SCAP). This
1436   data informs automation of vulnerability management, security measurement, and compliance. NVD
1437   includes databases of security checklists, security related software flaws, misconfigurations, product
1438   names, and impact metrics.

1439   **Non-vendor-directed:** This term is used to indicate that any sample chosen for testing is selected by the
1440   testing laboratory without the input or knowledge of the product vendor.

1441   **OVAL ID:** An identifier for a specific OVAL definition that conforms to the format for OVAL IDs. For
1442   more information please see the OVAL specification reference in Section 2.

1443   **Product:** A software application that has one or more capabilities.

1444   **Module (SCAP Module):** it is an embedded software component of a product or application, or a
1445   complete product in-and-of-itself that has one or more capabilities.

1446   **Product Output:** Information produced by a product. This includes the product user interface, human-
1447   readable reports, and machine-readable reports. Unless otherwise indicated by a specific requirement,
1448   there are no constraints on the format. When this output is evaluated in a test procedure, either all or
1449   specific forms of output will be sampled as indicated by the test procedure.

1450   **SCAP Capability:** A specific function or functions of a product as defined below:

1451   ■   Authenticated Configuration Scanner: the capability to audit and assess a target system to determine
1452   its compliance with a defined set of configuration requirements using target system logon privileges.

1453   ■   Common Vulnerabilities and Exposures (CVE) Option: the capability to process and present CVEs
1454   correctly and completely

1455   ■   Open Checklist Interactive Language (OCIL) Option: the capability to process and present OCIL
1456   correctly and completely

1457   **SCAP Component:** One of the eleven specifications that comprise SCAP: Asset Identification, ARF,
1458   CCE, CCSS, CPE, CVE, CVSS, OCIL, OVAL, TMSAD, and XCCDF.

1459   **SCAP Result Data Stream:** A bundle of SCAP components, along with the mappings of references
1460   between SCAP components, that holds output (result) content.

1461   **SCAP Revision:** A version of the SCAP specification designated by a revision number in the format
1462   nn.nn.nn, where the first nn is the major revision number, the second nn number is the minor revision
1463   number, and the final nn number is the refinement number. A specific SCAP revision will populate all
1464   three fields, even if that means using zeros to show no minor revision or refinement number has been
1465   used to date. A leading zero will be used to pad single-digit revision or refinement numbers.

1466   **SCAP Source Data Stream:** A bundle of SCAP components, along with the mappings of references
1467   between SCAP components, that holds input (source) content. See also Compliance Mapping.

1468   **Software Flaw:** See Vulnerability.

1469   **Target Platform:** The target operating system or application on which a vendor product will be
1470   evaluated using a platform-specific validation lab test suite. These platform-specific test suites consist of
1471   specialized SCAP content used to perform the test procedures defined in this document.

1472   **Tier I Checklist:** A checklist in the National Checklist Repository that is prose-based, such as narrative
1473   descriptions of how a person can manually alter a product's configuration.

1474   **Tier II Checklist:** A checklist in the National Checklist Repository that documents the recommended
1475   security settings in a machine-readable but non-standard format, such as a proprietary format or a
1476   product-specific configuration script.

1477   **Tier III Checklist:** A checklist in the National Checklist Repository that uses SCAP to document the
1478   recommended security settings in machine-readable standardized SCAP formats that meet the definition
1479   of "SCAP Expressed" specified in NIST SP 800-126. SCAP Validated products should be able to process
1480   Tier III checklists.

1481   **Tier IV Checklist:** A checklist in the National Checklist Repository that is considered production-ready
1482   and has been validated by NIST or a NIST-recognized authoritative entity to ensure, to the maximum
1483   extent possible, interoperability with SCAP-validated products. Tier IV checklists also demonstrate the
1484   ability to map low-level security settings (for example, standardized identifiers for individual security
1485   configuration issues) to high-level security requirements as represented in various security frameworks
1486   (e.g., SP 800-53 controls for FISMA), and the mappings have been vetted with the appropriate authority.

1487   **Vulnerability:** An error, flaw, or mistake in computer software that permits or causes an unintended
1488   behavior to occur. CVE is a common means of enumerating vulnerabilities.

1489   **XCCDF Content:** A file conforming to the XCCDF schema. For more information please see the
1490   XCCDF specification reference in Section 2.

Appendix B—Acronyms

This appendix contains selected acronyms and abbreviations used in the publication.

ACS	Authenticated Configuration Scanner	
ARF	Asset Reporting Format	
CCE	Common Configuration Enumeration	
CCSS	Common Configuration Scoring System	
CPE	Common Platform Enumeration	
CVE	Common Vulnerabilities and Exposures	
CVSS	Common Vulnerability Scoring System	
DTR	Derived Test Requirement	
FDCC	Federal Desktop Core Configuration	
FIRST	Forum of Incident Response and Security Teams	
FISMA	Federal Information Security Management Act	
GUI	Graphical User Interface	
HTML	Hypertext Markup Language	
ID	Identifier	
IETF	Internet Engineering Task Force	
IR	Interagency Report	
IT	Information Technology	
ITL	Information Technology Laboratory	
NCP	National Checklist Program	
NIST	National Institute of Standards and Technology	
NSA	National Security Agency	
NVD	National Vulnerability Database	
NVLAP	National Voluntary Laboratory Accreditation Program	
OCIL	Open Checklist Interactive Language	
OCIL QI	Open Checklist Interactive Language Questionnaire Interpreter	
OMB	Office of Management and Budget	
OS	Operating System	
OVAL	Open Vulnerability and Assessment Language	
OVAL DI	Open Vulnerability and Assessment Language Definition Interpreter	
PDF	Portable Document Format	
RFC	Request for Comment	
RHEL	Red Hat Enterprise Linux	
SCAP	Security Content Automation Protocol	
SCAPVal	SCAP Validation tool	
SP	Special Publication	
TMSAD	Trust Model for Security Automation Data	
URI	Uniform Resource Identifier	
URL	Uniform Resource Locator	
U.S.	United States	
USGCB	United States Government Configuration Baseline	
WFN	Well-Formed Name	
XCCDF	Extensible Configuration Checklist Document Format	
XML	Extensible Markup Language	

Appendix C—Use of SCAP 1.2 Logo and phrases

1538

1539   This appendix contains information regarding the use of SCAP 1.2 Logo and phrases
1540
1541
1542   The phrases SCAP 1.2 Validated and SCAP 1.2 Logo are intended for use in association with SCAP 1.2
1543   products or modules validated by the National Institute of Standards and Technology (NIST) as
1544   complying with Security Content Automation Protocol (SCAP) Version 1.2 Requirements for
1545   Products/Modules.
1546
1547   Vendors of validated SCAP products and/or modules or vendors of products that embed validated SCAP
1548   modules are encouraged to use the phrases and logo provided that they agree to the following and
1549   returning the signed SCAP 1.2 Logo Form:
1550
1551   1. The phrases SCAP 1.2 Validated and the SCAP 1.2 Logo are Certification Marks of NIST, which
1552   retains exclusive rights to their use.
1553
1554   2. NIST reserves the right to control the quality of the use of the phrase SCAP 1.2 Validated and the
1555   logo itself.
1556
1557   3. Permission for advertising SCAP 1.2 validation and use of the logo is conditional on and limited
1558   to those SCAP products/modules validated by NIST as complying with the requirements for
1559   Security Content Automation Protocol (SCAP) Version 1.2.
1560
1561   4. An SCAP module may either be a component of a product, or a standalone product. Use of the
1562   SCAP 1.2 Logo on product reports, letterhead, brochures, marketing material, and product
1563   packaging shall be accompanied by the following: 'TM: A Certification Mark of NIST, which
1564   does not imply product endorsement by NIST or the U.S. Government'. If the SCAP module is a
1565   component of a product, the phrase "SCAP 1.2 Inside" shall accompany the logo.
1566
1567   5. Permission for the use of the phrase SCAP 1.2 Validated and the logo may be revoked at the
1568   discretion of NIST.
1569
1570   6. Permission to use the phrase SCAP 1.2 Validated and the SCAP 1.2 Logo in no way constitutes
1571   or implies product endorsement by NIST.
1572

Appendix D—References

1573

1574   The following references are cited in the document above.

1575

[FIPS 140-2]	Federal Information Process Standards Publication (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, May 2001 (with Change Notices through December 3, 2002). http://csrc.nist.gov/publications/PubsFIPS.html#140-2.
[NIST HB 150]	NIST Handbook 150 (2006 Edition), *National Voluntary Laboratory Accreditation Program: Procedures and General Requirements*, February 2006. http://www.nist.gov/nvlap/upload/nist-handbook-150.pdf.
[NIST HB 150-17]	NIST Handbook 150-17, *NVLAP Cryptographic and Security Testing*, May 2013. http://dx.doi.org/10.6028/NIST.HB.150-17.
[NISTIR 7275 R4]	NIST Interagency Report (NISTIR) 7275 Revision 4, *Specification for the Extensible Configuration Checklist Description Format (SCCDF) Version 2.1*, September 2011 (updated March 2012). http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7275-Rev.%204.
[NISTIR 7435]	NIST Interagency Report (NISTIR) 7435, *The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems*, August 2007. http://csrc.nist.gov/publications/nistir/ir7435/NISTIR-7435.pdf.
[NISTIR 7502]	NIST Interagency Report (NISTIR) 7502, *The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities*, December 2010. http://csrc.nist.gov/publications/nistir/ir7502/nistir-7502_CCSS.pdf.
[NISTIR 7511 R3]	NIST Interagency Report (NISTIR) 7511 Revision 3, *Security Content Automation Protocol (SCAP) Version 2.1 Validation Program Test Requirements*, January 2013 (updated July 11, 2013). http://dx.doi.org/10.6028/NIST.IR.7511.
[NISTIR 7692]	NIST Interagency Report (NISTIR) 7692, *Specification for the Open Checklist Interactive Language (OCIL) Version 2.0*, April 2011. http://csrc.nist.gov/publications/nistir/ir7692/nistir-7692.pdf.
[NISTIR 7693]	NIST Interagency Report (NISTIR) 7693, *Specification for Asset Identification 1.1*, June 2011. http://csrc.nist.gov/publications/nistir/ir7693/NISTIR-7693.pdf.
[NISTIR 7694]	NIST Interagency Report (NISTIR) 7694, *Specification for the Asset Reporting Format 1.1*, June 2011. http://csrc.nist.gov/publications/nistir/ir7694/NISTIR-7694.pdf.
[NISTIR 7695]	NIST Interagency Report (NISTIR) 7695, *Common Platform Enumeration: Naming Specification Version 2.3*, August 2011. http://csrc.nist.gov/publications/nistir/ir7695/NISTIR-7695-CPE-Naming.pdf.
[NISTIR 7696]	NIST Interagency Report (NISTIR) 7696, *Common Platform Enumeration: Name Matching Specification Version 2.3*, August 2011. http://csrc.nist.gov/publications/nistir/ir7696/NISTIR-7696-CPE-Matching.pdf.

[NISTIR 7697]   NIST Interagency Report (NISTIR) 7697, *Common Platform Enumeration: Dictionary Specification Version 2.3*, August 2011.
http://csrc.nist.gov/publications/nistir/ir7696/NISTIR-7696-CPE-Matching.pdf.

[NISTIR 7698]   NIST Interagency Report (NISTIR) 7698, *Common Platform Enumeration: Applicability Language Specification Version 2.3*, August 2011.
http://csrc.nist.gov/publications/nistir/ir7698/NISTIR-7698-CPE-Language.pdf.

[NISTIR 7802]   NIST Interagency Report (NISTIR) 7802, *Trust Model for Security Automation Data 1.0 (TMSAD)*, September 2011.
http://csrc.nist.gov/publications/nistir/ir7802/NISTIR-7802.pdf.

[NIST SP 800-53 R4] NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated January 22, 2015).
http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[NIST SP 800-126 R1] NIST Special Publication (SP) 800-126 Revision 1, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1*, February 2011.
http://csrc.nist.gov/publications/nistpubs/800-126-rev1/SP800-126r1.pdf.

[NIST SP 800-126 R2] NIST Special Publication (SP) 800-126 Revision 2, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*, September 2011.
http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf.

[OMB M-08-22]   Office of Management and Budget (OMB) Memorandum M-08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)*, August 11, 2008.
http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-22.pdf

[RFC 2119]   Internet Engineering Task Force (IETF) Request for Comment (RFC) 2119, *Key words for use in RFCs to Indicate Requirement Levels*, March 1997.
http://www.ietf.org/rfc/rfc2119.txt.

[XMLS]   World Wide Web Consortium (W3C) Recommendation, *XML Schema* [XML Schema 1.1], October 28, 2004.
http://www.w3.org/XML/Schema.html.

1576